UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

BRUNA SARDAGNA SUDOSKI

UM ESTUDO DE CASO DE DESENVOLVIMENTO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO, COM BASE NAS NORMAS ABNT NBR ISO/IEC:27000, PARA UMA INSTITUIÇÃO DE SOLUÇÕES TECNOLÓGICAS

Florianópolis
2017
Bruna Sardagna Sudoski

UM ESTUDO DE CASO DE DESENVOLVIMENTO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO, COM BASE NAS NORMAS ABNT NBR ISO/IEC:27000, PARA UMA INSTITUIÇÃO DE SOLUÇÕES TECNOLÓGICAS

Trabalho de conclusão de curso apresentado como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de informação.

Orientador(a): Prof. Dra.Carla Merkle Westphall

Florianópolis
2017

Dedico este trabalho à minha mãe Inês e ao meu pai Sérgio, por todo apoio e esforço para me proporcionar as oportunidades que me permitiram chegar até aqui, aos meus amigos Bianca, Fernanda e Guilherme, que me acompanharam durante esta grande caminhada acadêmica, e à Gabriella, por todo o amor e conforto durante os momentos de dificuldade.

“Faça o melhor que puder, no tempo que tiver, da maneira que conseguir, e compreenda que além disto já não está no seu controle.”

(Daniel Duarte)

RESUMO

Evidencia-se constantemente, através da literatura e de exemplos práticos reais, que a informação é um dos bens mais preciosos dentro de uma organização. Considerando isso, através da aplicação de medidas de proteção, mitigação e contingência para software e hardware, as organizações buscam manter suas informações com o maior grau de segurança possível. Dentre a gama de alternativas para se garantir essa segurança, o desenvolvimento e aplicação de uma Política de Segurança da Informação (PSI) é uma das ferramentas de grande auxílio para garantir a segurança em um ambiente organizacional específico. Para auxiliar na padronização, confiança e na qualidade dessas PSI, usa-se como diretriz para o seu desenvolvimento uma ou mais normas. Um exemplo de norma utilizadas para esse fim, é a família de norma ABNT NBR ISO/IEC 27000, utilizada entre as organizações brasileiras para alcançar excelência na segurança da informação através da sua adaptação para suas respectivas PSI. O presente trabalho, portanto, visa realizar um estudo de caso em um laboratório que desenvolve soluções tecnológicas, avaliando e analisando o contexto do ambiente, e desenvolvendo uma PSI para o mesmo, com base nas normas da família ABNT NBR ISO/IEC 27000.

Palavras-chave: Política de segurança da informação, Segurança da informação, Normas, ABNT NBR ISO/IEC 27000

ABSTRACT

It is constantly shown through literature and real practical examples that information is one of the most precious assets within an organization. Considering this, through the application of protection, mitigation and contingency measures for software and hardware, organizations seek to keep their information as safe as possible. Among the range of alternatives to ensure such security, the development and application of an Information Security Policy (ISP) is one of the tools that helps to ensure security in a specific organizational environment. To help in the standardization, confidence and quality of these ISP, one or more standards are used as guidelines for its development. An example of standards used for this purpose are the ABNT NBR ISO/IEC 27000 family of standards used among Brazilian organizations to achieve excellence in information security by adapting it to their respective ISPs. The present work, therefore, aims to carry out a case study in a institution that develops technological solutions, evaluating and analyzing the context of the environment, and developing a PSI for it, based on the ABNT NBR ISO / IEC 27000 family standards.

Key-words: Information Security Police, Information Security, Standards, ABNT NBR ISO/IEC 27000

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT - Associação Brasileira de Normas Técnicas
AMN - Associação Mercosul de Normalização
ANVISA - Agência Nacional de Vigilância Sanitária
ASTM - *American Society for Testing and Materials*
CEN - Comitê Europeu de Normalização
CID - Confiabilidade, Integridade, Disponibilidade
IEC - International Electrotechnical Commission
ISO - International Organization for Standardization Organização Internacional de Normalização
NBR - Denota uma norma brasileira emitida pela ABNT
OWASP - *Open Application Security Project*
PSI - Políticas de Segurança da Informação
SGSI - Sistema de Gestão de Segurança da Informação
PDCA - *Plan-Do-Check-Act*

SUMÁRIO

1. INTRODUÇÃO

A informação é vital para uma organização, por isso garantir a segurança da informação auxilia uma organização a proteger seus recursos financeiros e físicos, bem como sua reputação, posição legal, empregados entre outros ativos tangíveis e intangíveis (HUMPHREYS, 2005; PELTIER, 2012). De acordo com (PELTIER, 2012), definir normas e políticas de segurança da informação deve ser a primeira ação que toda organização deveria executar para se proteger de riscos de segurança.

Segundo (DISTERER, 2013), essas normas de segurança da informação “podem ser usadas como diretriz ou estrutura para desenvolver e manter uma gestão adequada de segurança da informação”. O autor afirma ainda que elas “representam um consenso sobre características como qualidade, segurança e confiabilidade, que devem permanecer aplicáveis por um longo período de tempo”.

A International Organization of Standardization (ISO) é responsável pelo desenvolvimento de centenas de normas internacionais, que cobrem áreas de tecnologia e indústria (International Organization of Standardization, ISO Story). Dentre as normas desenvolvidas por esta organização, tem-se a família ISO/IEC 27000, que compreende um conjunto de padrões voltados para a segurança da informação, descrevendo termos, objetivos de controle, requisitos e diretrizes, com as quais organizações podem alcançar segurança de informação (DISTERER, 2013). Essa família de normas podem ser aplicadas para diferentes portes e perfis organizacionais, como por exemplo empresas comerciais, agências governamentais e organizações sem fins lucrativo. (International Organization of Standardization, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary). No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) adota os padrões desta família de normas, adaptando-as e traduzindo-as para português, que compõem, então, a família ABNT NBR ISO 27000.

Por serem desenvolvidas visando a adaptabilidade em diferentes tipos de ambientes, essas normas apresentam uma visão generalizada de como garantir a segurança da informação. Por este motivo, é necessário que cada ambiente realize uma avaliação de como a segurança da informação deve ser tratada especificamente

para o ambiente em questão. As Políticas de Segurança da Informação (PSI) são o tipo de documentação a serem desenvolvidas neste caso, pois segundo (CALDER, 2016), elas devem capturar a realidade organizacional do ambiente, juntamente com os requerimentos definidos em normas a serem consideradas.

Considerando a importância de se garantir a segurança da informação, e o uso de normas e políticas de segurança da informação para atingir esse objetivo, o presente trabalho visa realizar um estudo mais aprofundado referente à conceitos e à usabilidade de normas e políticas, e aplicar este estudo no desenvolvimento de PSI para um ambiente real, tendo em vista que o mesmo carece de uma PSI em vigor atualmente.

2. OBJETIVOS

2.1 Objetivo Geral

O objetivo geral deste projeto é realizar um estudo de caso em um ambiente real, que desenvolve soluções tecnológicas, analisando e desenvolvendo uma Política de Segurança da Informação para o mesmo, uma vez que este ambiente não possui atualmente uma PSI em vigência.

2.2 Objetivos Específicos

Fazem parte dos objetivos específicos deste trabalho:

01. Sintetizar a fundamentação teórica e o estado da arte acerca de conceitos de segurança da informação, riscos, vulnerabilidades, ameaças, ferramentas de segurança, Políticas de Segurança da Informação e normas da família ISO/IEC 27000 e ABNT NBR ISO/IEC 27000;
02. Levantar dados referente ao ambiente na qual o estudo de caso será aplicado, através de entrevistas e encontros com membros do local a ser estudado;
03. Realizar, a partir dos dados coletados, uma análise do ambiente, organizando e classificando o que será abordado na PSI a ser desenvolvida;
04. Realizar o desenvolvimento, a partir dos dados coletados e avaliados, uma PSI em conformidade com normas selecionadas da família ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISO/IEC 27005:2011;

3. FUNDAMENTAÇÃO TEÓRICA

3.1 Classificação da Informação

Segundo a ABNT (2013, p. 25), as informações devem ser classificadas de acordo com seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada. A fonte afirma ainda que essa classificação visa “Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.”. Através dessa classificação, é possível que os responsáveis possam lidar com informações e tenham maior noção de como tratar e proteger essas informações.

Atualmente, existem diversos esquemas de classificações adotadas por autores da literatura. Para WHITMAN e MATTORD (2011) as informações podem ser classificadas nas seguintes categorias:

- Confidencial: Esta classificação engloba as informações mais sensíveis da organização, necessitando um controle mais restrito de acesso e manipulação das mesmas, que deve ser restrito a indivíduos específicos da organização, ou sob requerimentos de termos ou contratos.
- Interna: Classificação utilizada para todas as informações que não se enquadram como Confidenciais, e podem ser acessadas apenas por membros internos da organização, indivíduos autorizados ou terceiros.
- Externa: Toda informação que tenha sido aprovada pela gerência para divulgação pública.

Existe, também, um esquema de classificação de informações comumente utilizado por instituições que necessitam de um tratamento mais sensível e rigoroso, como por exemplo as instituições militares (STALLINGS, 2008), (STAMP, 2011), (WHITMAN e MATTORD, 2011):

- Top Secreta: Informações cuja divulgação pode trazer consequências extremamente ruins para a segurança nacional. Para um indivíduo adquirir

acesso a estas informações, o mesmo deve passar por uma rigorosa análise de cenário, possivelmente incluindo entrevistas, análises com polígrafos, exames de perfil psicológico, entre outros.

- Secreta: Informações cuja divulgação pode trazer consequências ruins para a segurança nacional. Para a aquisição destas informações, um indivíduo deve passar por um procedimento de análise de cenário mais amena, em comparação com as análises realizadas para as informações Top Secretas.
- Confidencial: Informações cuja divulgação pode causar danos para a segurança nacional.
- Não Classificada: Informações que podem ser divulgadas publicamente, sem que isto represente danos à segurança nacional.

Já DIAS (2000) propõe o seguinte esquema de classificação em quatro níveis:

- Secreta: Informações cujo acesso é restrito à apenas alguns indivíduos e, por se tratarem de informações sensíveis à organização, seu controle deve ser total. O acesso externo ou interno é crítico para a instituição.
- Confidencial: Informações de acesso exclusivo ao ambiente da organização, porém seu acesso é realizado apenas quando necessário, ou quando for fundamental para que indivíduos possam desempenhar suas funções. O acesso externo é crítico para a instituição.
- Interna: Informações que devem ser acessadas apenas internamente da organização. Entretanto, caso ocorra o acesso externo, as consequências não são consideradas críticas.
- Públicas: Estas informações podem ser divulgadas publicamente.

Estes exemplos de esquemas apresentados podem e são utilizados por organizações do mundo real, entretanto, a classificação de informações é algo flexível, possibilitando que as organizações criem e adaptem esquemas de acordo com suas necessidades específicas. Para o escopo deste projeto, será utilizada a classificação de informações definida por WHITMAN e MATTORD (2011).

3.2 Características da Segurança da Informação

WHITMAN e MATTORD (2011, p. 11) citam que “o valor da informação reside nas características que as mesmas possuem”. Considerando isto, existem três características da segurança da informação, conhecidas como a tríade “CID” (Confidencialidade, Integridade e Disponibilidade), que uma vez preservadas, asseguram o valor e a segurança da informação. Estas características são:

- Confidencialidade: Para WHITMAN e MATTORD (2011, p. 13), a confidencialidade da informação é garantida quando a mesma “está protegida da divulgação ou exposição a indivíduos ou sistemas não autorizados”. Desta maneira, a confidencialidade garante que uma informação será acessada apenas por aqueles que possuam privilégios e direitos para acessá-la.
- Disponibilidade: Segundo COELHO, ARAÚJO e BEZERRA (2014, p. 7), a disponibilidade “determina que recursos estejam disponíveis para acesso, por entidades autorizadas, sempre que solicitadas”. Sendo assim, a informação perde esta característica quando usuários autorizados encontram interrupções, obstáculos ou demais impedimentos durante a tentativa de acesso a informação.
- Integridade: A integridade da informação é a garantia de que a mesma será recebida exatamente da maneira que foi enviada por uma entidade autorizada. Sendo assim, integridade assegura que a informação não sofreu modificação, inserção, exclusão ou repetição (STALLINGS, 2008).

A medida que a tecnologia avançou, as ameaças à segurança da informação tornaram-se mais sofisticadas, atingindo o ponto em que, para garantir um maior grau de segurança, necessita-se considerar outros conceitos, além dos abordados na tríade CID. Dentre os diversos conceitos considerados na literatura atual, considerando o escopo do presente projeto, é necessário definir apenas os seguintes:

- Controle de acesso: Segundo STALLINGS (2008), este conceito se refere ao controle de quem pode ter acesso a informação, sob quais condições o acesso pode ocorrer e o que é permitido para aqueles que acessam a informação.

COELHO, ARAÚJO e BEZERRA (2014) acrescentam que este controle pode ser exercido através de processos de identificação, autenticação e autorização.

- Posse: Para WHITMAN e MATTORD (2011, p. 15), a posse da informação refere-se a qualidade ou estado de propriedade ou controle. Os autores ainda acrescentam:

> "[...] a informação está na posse de um indivíduo, se o mesmo a obtiver, independente do formato ou outras características. Embora uma violação da confidencialidade resulte sempre em uma violação da posse, uma violação da posse nem sempre resulta em violação da confidencialidade."

3.3 Segurança da Informação

COELHO, ARAÚJO e BEZERRA (2014, p. 2) definem segurança da informação da seguinte maneira:

> "Segurança da informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança."

Esta proteção de ativos mencionada, é detalhada por WHITMAN e MATTORD (2011, p. 181) como "proteger a confidencialidade, integridade e disponibilidade de ativos de segurança, seja no armazenamento, processamento ou transmissão" destes. Ainda segundo os mesmos autores (2011, p. 181), a segurança da informação "é alcançada através da aplicação de políticas, educação, treinamento, conscientização e tecnologia".

É possível observar, que tanto COELHO, ARAÚJO e BEZERRA (2014) quanto WHITMAN e MATTORD (2011), mencionam o conceito de ativos, quando abordam sobre segurança da informação. Para tanto, conceitua-se ativos como qualquer coisa que possua valor para uma organização e seus negócios. Desta forma, ativos podem

ser, por exemplo, produtos, serviços, equipamentos e pessoas, como mostra a Figura 1.

Figura 1: Exemplos de Ativos de Informação

Fonte: LYRA (2015)

Sendo assim, para COELHO, ARAÚJO e BEZERRA (2014), uma organização ou uma instituição que procura garantir a segurança da informação está, consequentemente, auxiliando na continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio.

O Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil (2016) realiza um levantamento anual de todos os incidentes de violação na segurança da informação reportados no Brasil. Este levantamento é apresentado na Figura 2, onde é possível observar um significativo aumento de incidentes reportados com o passar dos anos. Este tipo de estatística reforça a importância da segurança da informação nos dias atuais.

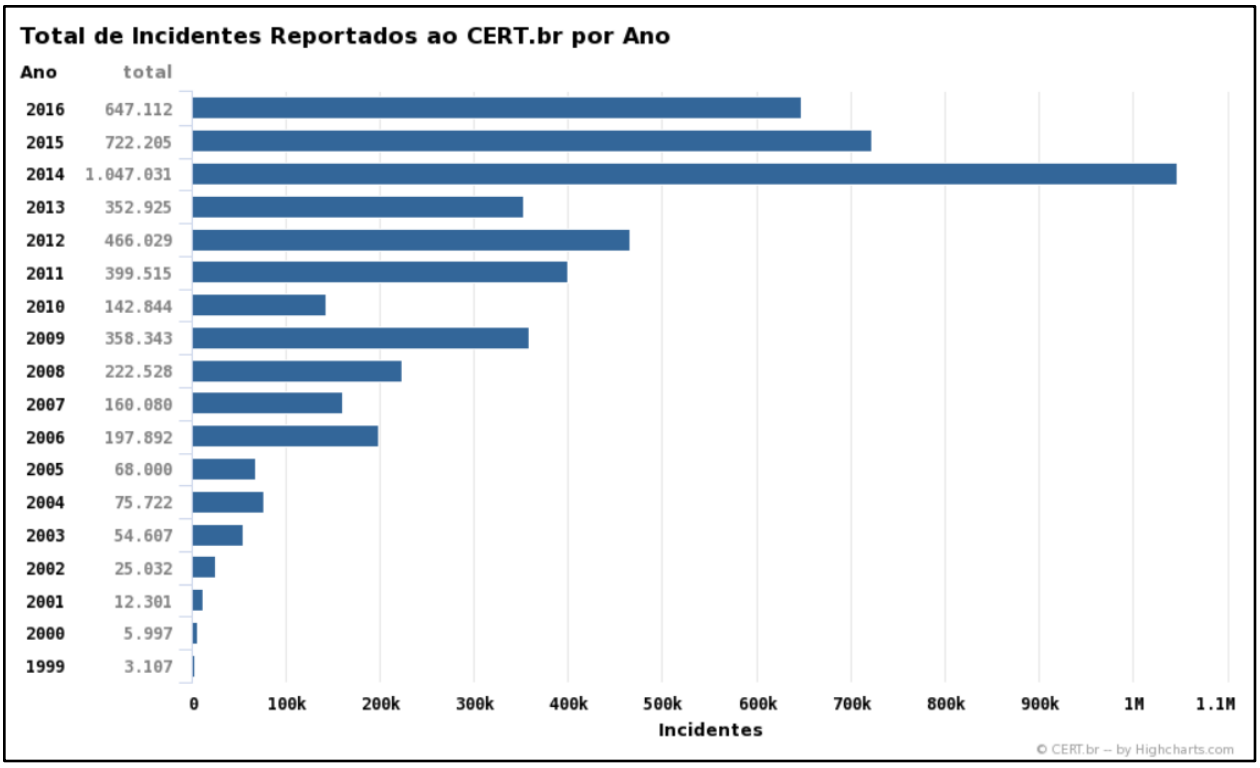

Figura 2: Total de Incidentes Reportados ao CERT.br Por Ano.

Fonte CERT.br (2016)

No estudo realizado pela DARYUS STRATEGIC RISK CONSULTING (2014), em 2014, é possível obter uma visão mais aprofundada de como a segurança da informação é tratada dentro das organizações:

- 52,46% dos sistemas de gestão de segurança da informação (SGSI) são informais ou inexistentes.
- 36,89% não possuem nenhum tipo de política de segurança da informação (PSI).
- 77,05% não possuem certificação ISO 27002.
- 63,63% não possuem um processo formal para gestão de incidentes de segurança da informação.
- 44,54% não possuem plano de continuidade de negócios.

Este comportamento é semelhante em outros países ao redor do mundo. Por exemplo, a EY (2017) realizou um estudo, entre 2016 e 2017, com líderes de empresas de diversos continentes, e obteve as seguintes estatísticas:

- 62% não aumentariam seus gastos de cibersegurança depois de experimentar uma violação que não causasse nenhum prejuízo.
- 49% não fazem ideia dos danos financeiros que um ciberataque causa ou pode causar.
- 57% dos entrevistados experimentaram um incidente de cibersegurança recente significativo.

Estes números reforçam a ideia de como a segurança da informação não é tratada com devida atenção pelas organizações. Um estudo realizado em 2015 pela PwD (2016), envolvendo 127 países, descreve que o valor médio de perdas financeiras relacionados a incidentes de segurança cibernética, considerando pequenas, médias e grandes empresas, chega a $2.450.000,00 ao ano. Estes dados são evidenciados com maiores detalhes na Figura 3.

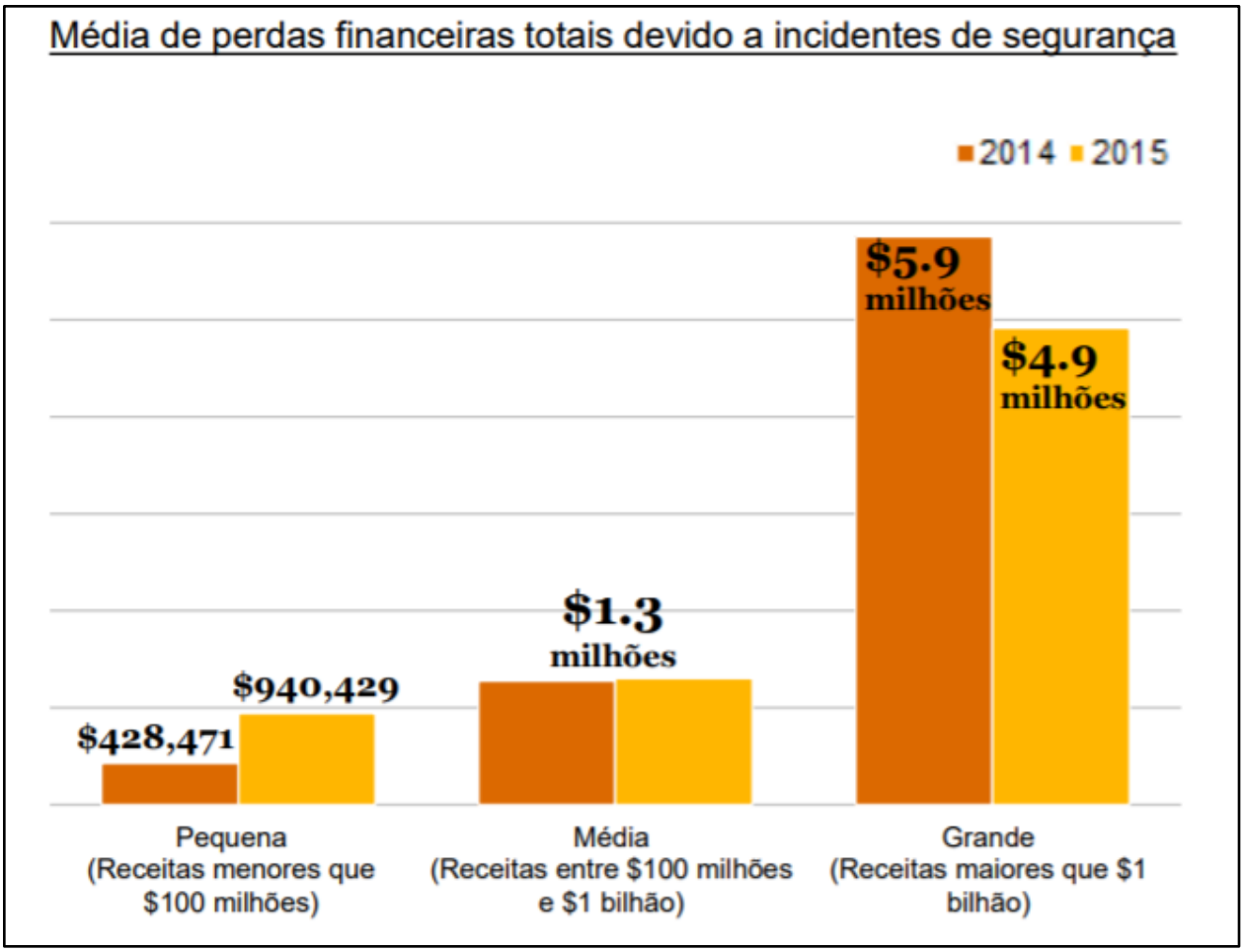

Figura 3: Média de perdas financeiras totais devido a incidentes de segurança

Fonte PwD (2016)

3.4. Riscos, Vulnerabilidades, Ataques e Ameaças

Ao lidar com o que pode prejudicar a segurança da informação e de ativos, algumas terminologias são abordadas. Riscos, vulnerabilidades, ameaças e ataques são mencionadas na literatura, e devem ser compreendidas para que seja possível proteger os ativos.

- Vulnerabilidade: É conceituado pela OWASP (2018), que vulnerabilidades são fraquezas no projeto, implementação, operação ou gerenciamento de um sistema, que possibilite que este ativo seja explorado e sua segurança violada. Diversas destas vulnerabilidades já foram examinadas, documentadas, e são de

conhecimento global, entretanto, muitas outras ainda permanecem desconhecidas (WHITMAN e MATTORD 2011).

- Ameaça: Conceitua-se ameaça como um evento, uma capacidade, ação, ou circunstância que pode causar incidentes indesejados em ativos e, consequentemente, danos para a organização (THE INTERNET SOCIETY 2000). Desta forma, ameaças são o que exploram as vulnerabilidades de ativos. WHITMAN e MATTORD (2011) acrescentam que estas ameaças estão sempre presentes, podendo ser intencionais ou não.
- Risco: Segundo COELHO, ARAÚJO e BEZERRA (2014), riscos consistem na combinação da probabilidade de um evento ocorrer e suas referentes consequências para a organização ou instituição. Desta maneira, pode-se concluir que os riscos são a probabilidade de uma ameaça explorar uma determinada vulnerabilidade de um ativo. Ainda, as organizações devem minimizar os riscos até o nível em que estes riscos se tornem aceitáveis para a mesma (WHITMAN e MATTORD 2011).
- Ataque: Um ataque é qualquer ação contra ativos que venha a comprometer a segurança de uma organização. Conclui-se, então, que ataques são ameaças concretizadas COELHO, ARAÚJO e BEZERRA (2014). Ataques podem ainda ser classificados como passivos ou ativos:
    - Passivos: Estes tipos de ataques consistem no monitoramento não autorizado de transmissões, visando obter as informações que são transmitidas. Ataques passivos não realizam alterações nas informações, e por este motivo são difíceis de detectar. Entretanto, é possível aplicar técnicas de defesa que auxiliem na prevenção deste tipo de ataque (COELHO, ARAÚJO e BEZERRA 2014).
    - Ativos: Diferentemente dos ataques passivos, os ataques ativos consistem em realizar modificações nas informações interceptadas, criando dados falsificados. Segundo COELHO, ARAÚJO e BEZERRA (2014), são ataques de difícil prevenção, por causa da necessidade de proteção completa de todas as facilidades de comunicação e processamento, durante o tempo todo.

3.5 Ferramentas de segurança

Atualmente existem diversas maneiras de lidar com a segurança da informação, diminuindo vulnerabilidades, e prevenindo que ataques ocorram, e até mesmo métodos que auxiliem a tomada de decisão efetiva caso um ataque venha a ocorrer ALSHAMMARI e BACH (2013). definem que estas técnicas podem ser classificadas entre controles físicos, administrativos e técnicos:

- Físico: Envolve a defesa de ativos físicos. ALSHAMMARI e BACH (2013) justificam a importância deste tipo de técnica de defesa, pois todo dano causado em equipamentos pode causar, também, perda de dados e informação, comprometendo a organização. A segurança física auxilia com que os sistemas de informação estejam seguros contra desastres naturais, falhas técnicas e humanas. Nesta categoria, temos como exemplos desta categoria: alarmes de segurança, sistemas de detecção de fumaça, trancas de portas, câmeras de segurança, blindagem, controle anti roubo, entre outros.

- Administrativos: Envolvem garantir a defesa da informação e ativos através da aplicação de medidas administrativas, que visam servir como regras ou guias de como pessoas e sistemas devem se comportar para garantir a segurança dos ativos de um ambiente. Temos como exemplos de técnicas para esta categoria: leis, regulamentos, políticas, guias, procedimentos, patentes, direitos autorais, contratos e acordos.

- Técnicos: Esta categoria envolve garantir a defesa da informação e ativos através do uso de tecnologia, ou seja, com a aplicação de hardware e software. Tem-se como exemplo do que pode ser utilizado como controle técnico: senhas e outros métodos de autenticação, protocolos de rede, firewalls, sistemas de detecção a intrusão, criptografia, reguladores de

tráfego de rede, programas ou sistemas operacionais que controlem acesso.

3.6 Normas

Segundo a Associação Brasileira de Normas Técnicas (ABNT),

> "Norma é o documento estabelecido por consenso e aprovado por um organismo reconhecido, que fornece regras, diretrizes ou características mínimas para atividades ou para seus resultados, visando à obtenção de um grau ótimo de ordenação em um dado contexto."

Normalmente, um ambiente que lida com sistemas de informações é complexo, incluindo uma variedade de sistemas de armazenamento, servidores, estações de trabalho, redes locais, Internet e outras conexões de rede remotas. Para os responsáveis dentro destes ambientes, garantir a segurança de ativos pode rapidamente se tornar uma tarefa extensa e complicada que, como já apresentado em capítulos anteriores, se não tratada com devida atenção, pode vir a trazer consequências desastrosas (STALLINGS, 2007).

Por este motivo, as normas que auxiliam a garantir a segurança da informação para instituições e organizações tem se tornado cada vez mais essenciais em tais circunstâncias. Para STALLING (2007), as normas podem servir para auxiliar a definir o escopo de funções e recursos de segurança necessários, de políticas de gerenciamento de informações e recursos humanos, de critérios para avaliar a eficácia das medidas de segurança, técnicas para avaliação contínua de segurança e monitoramento contínuo de violações de segurança e procedimentos para lidar com falhas de segurança.

Conforme explica a ABNT (2013), as normas podem ser desenvolvidas para serem aplicadas em diversos níveis de abrangência. Estes níveis podem ser representados como mostra a Figura 4.

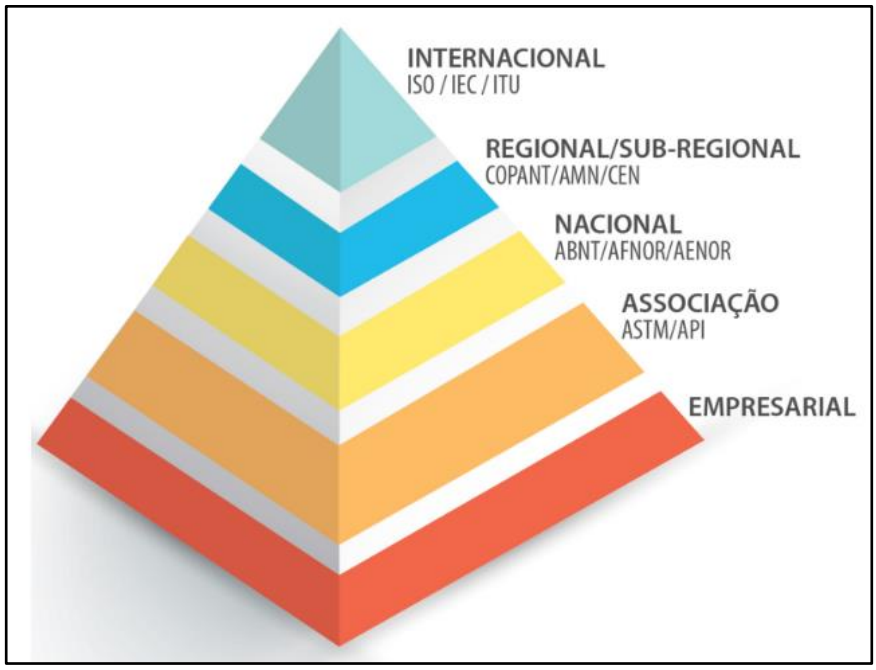

Figura 4: Níveis de Organização

Fonte: ABNT

- **Nível internacional:** Denominadas Normalização Internacional, normas deste nível tem abrangência mundial. Para tanto, devem ser desenvolvidas por uma Organização Internacional de Normalização. Normas ISO/IEC/ITU são exemplos de normas de nível internacional.

- **Nível regional:** Este nível de normalização abrange uma única região geográfica, econômica ou política do mundo, e são denominadas Normalização Regional. Devem ser estabelecidas por uma Organização Regional ou Sub-Regional de Normalização, para aplicação em um conjunto de países de uma região. Como exemplos de normas neste nível, tem-se as Normas da Associação Mercosul de Normalização (AMN) ou Comitê Europeu de Normalização (CEN).

- **Nível nacional:** Denominadas Normalização Nacional, esta categoria de normas são elaboradas pelas partes interessadas de um único país, seja governo, indústrias, consumidores ou comunidade científica de um país. Devem

posteriormente ser emitidas por um Organismo Nacional de Normalização, reconhecido como autoridade para torná-las públicas. Como exemplo de Normas Nacionais, tem-se as Normas da Associação Brasileira de Normas Técnicas (ABNT) ou Associação Alemã de Normas Técnicas (DIN).

- **Nível empresarial:** Normas deste nível são elaboradas por uma empresa ou grupo de empresas com o propósito de orientar as compras, a fabricação, as vendas e outras operações. Como exemplo desta categoria, tem-se as Normas Petrobrás ou procedimentos de gestão de qualidade.

- **Nível de associação:** Esta categoria de normalização abrange normas desenvolvidas no contexto de entidades associativas e técnicas, para o uso de seus associados. Podem, entretanto, ter seu uso expandido, tornando-se referência em uma esfera comercial ou industrial, por exemplo. Um exemplo deste tipo de norma, seria a *American Society for Testing and Materials* (ASTM).

Quando se trata de normas voltadas para segurança da informação, a referência de nível internacional com maior relevância atualmente é a norma ISO/IEC 17799, reeditada como ISO 27002, na então nova família ISO 27000 de normas de segurança. Resumidamente, DISTERER (2013) define que esta norma visa prover objetivos de controle, controles específicos, requisitos e diretrizes, com os quais a empresa ou organização pode obter uma segurança de informações adequada. O autor ainda afirma que ao buscar estar em conformidade com estas normas, uma organização promove a confiança entre clientes, além de reduzir o risco de multas ou pagamentos de compensação como resultado de disputas legais, uma vez que requisitos legais, como provisionamento, podem ser combatidos com a conformidade com padrões.

Segundo definido na norma ISO/IEC 27002, existem 11 (onze) seções de controle de segurança da informação. Embora as organizações possuam diferenças entre si, é recomendável que, se cabível, todas estas seções sejam consideradas. Desta forma, convém que cada organização que utilize esta norma identifique quais são as seções aplicáveis, quão importantes elas são e a sua aplicação para os

processos específicos do negócio. Abaixo são definidas cada uma destas 11 (onze) seções, de acordo com ISO/IEC 27002.

- **Política de segurança da informação**: Prover uma orientação e apoio a direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.
- **Organização da segurança da informação**: Gerenciar a segurança da informação dentro da organização, ou seja, manter a segurança das informações da organização e das instalações de processamento de informações que são acessadas, processadas, comunicadas ou gerenciadas por terceiros.
- **Gestão de ativos**: Alcançar e manter a proteção adequada dos ativos da organização.
- **Segurança em recursos humanos**: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades, estejam de acordo com os seus papéis, sejam adequados para a função que são designados e estejam cientes das ameaças e preocupações de segurança da informação.
- **Segurança física e do ambiente**: Prevenir o acesso físico não autorizado, danos e interferências nas instalações e informações da organização. Prevenir perdas, danos, roubo ou comprometimento de ativos físicos e interrupção das atividades da organização.
- **Gerenciamento das operações e comunicações**: Desenvolver controles para procedimentos operacionais, a fim de garantir a operação segura e correta dos recursos de processamento da informação.
- **Controle de acesso**: Controlar o acesso à informação através de controle de acesso à rede, controle de acesso ao sistema operacional, controle de acesso a aplicativos, controle de acesso a informações, entre outros requisitos de negócio.
- **Aquisição, desenvolvimento e manutenção de sistemas de informação**: Desenvolver controles para o processamento correto em

aplicativo através de funções criptográficas, segurança de arquivos do sistema, segurança do processo de suporte e gerenciamento de vulnerabilidades.

- **Gestão de incidentes de segurança da informação**: Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.
- **Gestão de continuidade de negócio**: Desenvolver abordagens que evitem a interrupção das atividades de negócios, protegendo processos críticos de negócios contra os efeitos de falhas ou desastres, garantindo assim sua retomada.
- **Conformidade**: Evitar violações de quaisquer leis, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação.

Atualmente, a família de normas 27000 abrange um total de 61 normas, das quais 52 já foram publicadas e 9 estão em desenvolvimento (International Organization for Standardization, 2018). Cada uma destas normas tem foco em um aspecto de segurança específico.

Na Figura 5, é apresentado um esquema da inter-relação entre as principais normas da família ISO IEC 27000, separadas em três níveis principais: Terminologias, Requisitos Gerais e Guias Gerais. Inicialmente, tem-se a nível de Terminologias a ISO 27000, que serve como contextualização da família 27000. Já o nível de Requisitos Gerais tem-se a ISO 27001, que contém requisitos que devem ser verificados para certificação de acordo com esta norma, e a ISO 27006, que contém os requisitos que devem ser cumpridos para que uma organização venha a ser credenciada como organização de certificação. A nível de Guias Gerais, são incluídos todas as demais normas, que podem ser considerados como diretrizes para diferentes domínios visando garantir a segurança da informação.

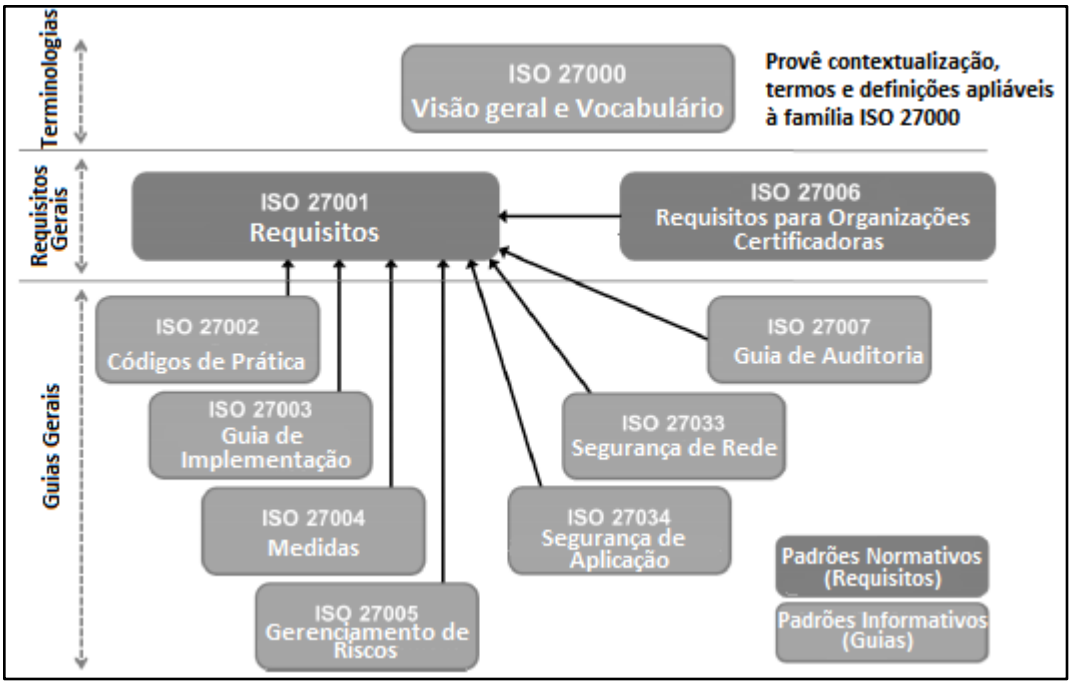

Figura 5: Inter relação entre as principais normas da família ISO 27000.
Fonte: ISO 27000

No Brasil, as normas ISO 27000 foram adaptadas pela Associação Brasileira de Normas Técnicas (ABNT), que gerou uma família de normas de nível nacional, denominadas ABNT NBR ISO IEC 27000. Considerando o escopo deste projeto, será levado em conta apenas três normas desta família: ABNT NBR ISO IEC 27001, ABNT NBR ISO IEC 27002 e ABNT NBR ISO IEC 27005:2011.

3.6.1 Norma ABNT NBR ISO IEC 27001:2013

Esta norma trata de aspectos que envolvem um Sistema de Gestão de Segurança da Informação (SGSI). Um SGSI consiste no resultado da aplicação planejada de objetivos, procedimentos, diretrizes, modelos, políticas e outras medidas administrativas que, conjuntamente, definem como são reduzidos os riscos para segurança da informação, dentro de uma instituição específica. A adoção de um SGSI deve ser uma decisão estratégica para uma organização e a especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização (ABNT, 2013).

Desta forma, é definido pela ABNT (2013), que a norma ISO 27001:

> "Especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização. Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes."

Esta norma pode ser utilizada para avaliação de conformidade interna ou externa, dependendo das partes interessadas e é através dela que uma organização pode obter a certificação em segurança da informação, assim assegurando que a organização possui competência e credibilidade em segurança de informação.

A norma segue as diretrizes da estratégia PDCA (*Plan*, *Do*, *Check*, *Act*), como definido na Figura 6. Nela, é ilustrado como um SGSI considera as entradas de requisitos de segurança da informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos e expectativas. Já na Tabela 1, é apresentado cada estado do PDCA ilustrado na Figura 6, com suas respectivas definições.

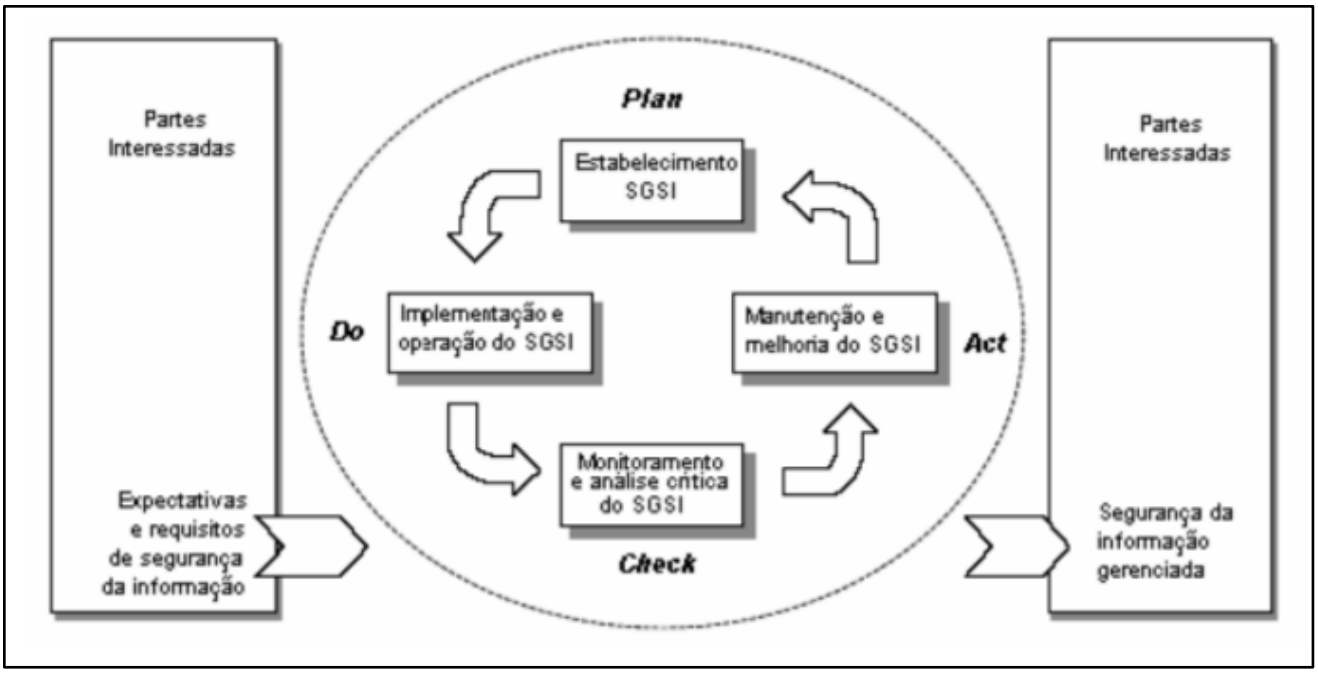

Figura 6 - Modelo PDCA aplicado aos processos do SGSI
Fonte: ABNT NBR ISO/IEC 27001:2013

Estado	Definição
Plan (planejar) (estabelecer o SGSI)	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.

Do (fazer) (implementar e operar o SGSI)	Implementar e operar a política, controles, processos e procedimentos do SGSI.
Check (checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
Act (agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Tabela 1: Modelo PDCA aplicado aos processos do SGSI
Fonte: ABNT NBR ISO/IEC 27001

É definido pela norma ABNT NBR ISO IEC 27001, que o SGSI deve ser planejado, implementado, monitorado, analisado e aperfeiçoado. Isto significa que a gestão tem suas responsabilidades definidas, que os objetivos devem ser estabelecidos, medidos e analisados, que deve haver auditorias internas, entre outros requisitos. Todos estes requisitos estão especificados nas 7 seções que compreendem a ABNT NBR ISO IEC 27001:

- Contexto da organização;
- Liderança;
- Planejamento;
- Apoio;
- Operação;
- Avaliação do desempenho;
- Melhoria.

3.6.2 Norma ABNT NBR ISO IEC 27002:2013

Enquanto a norma ABNT NBR ISO IEC 27001 define os requisitos para um Sistema de Gestão da Segurança da Informação e é a norma que uma organização deve utilizar como base para obter a certificação empresarial em gestão da segurança da informação, a norma ABNT NBR ISO IEC 27002:2013, apresenta um código de práticas com um conjunto completo de controles que auxiliam a aplicação do Sistema de Gestão da Segurança da Informação nas organizações e tem como objetivo estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. De maneira simplificada, pode-se dizer que a norma ABNT NBR ISO IEC 27001 gerencia o SGSI como um todo, enquanto a ABNT NBR ISO IEC 27002:2013 especifica aspectos que auxiliam o SGSI a ser mais robusto.

De acordo com COELHO, ARAÚJO e BEZERRA (2014, p. 20), os controles da norma são apresentados como boas práticas para que a organização adote uma postura preventiva e pró ativa diante das suas necessidades e requisitos de segurança da informação.

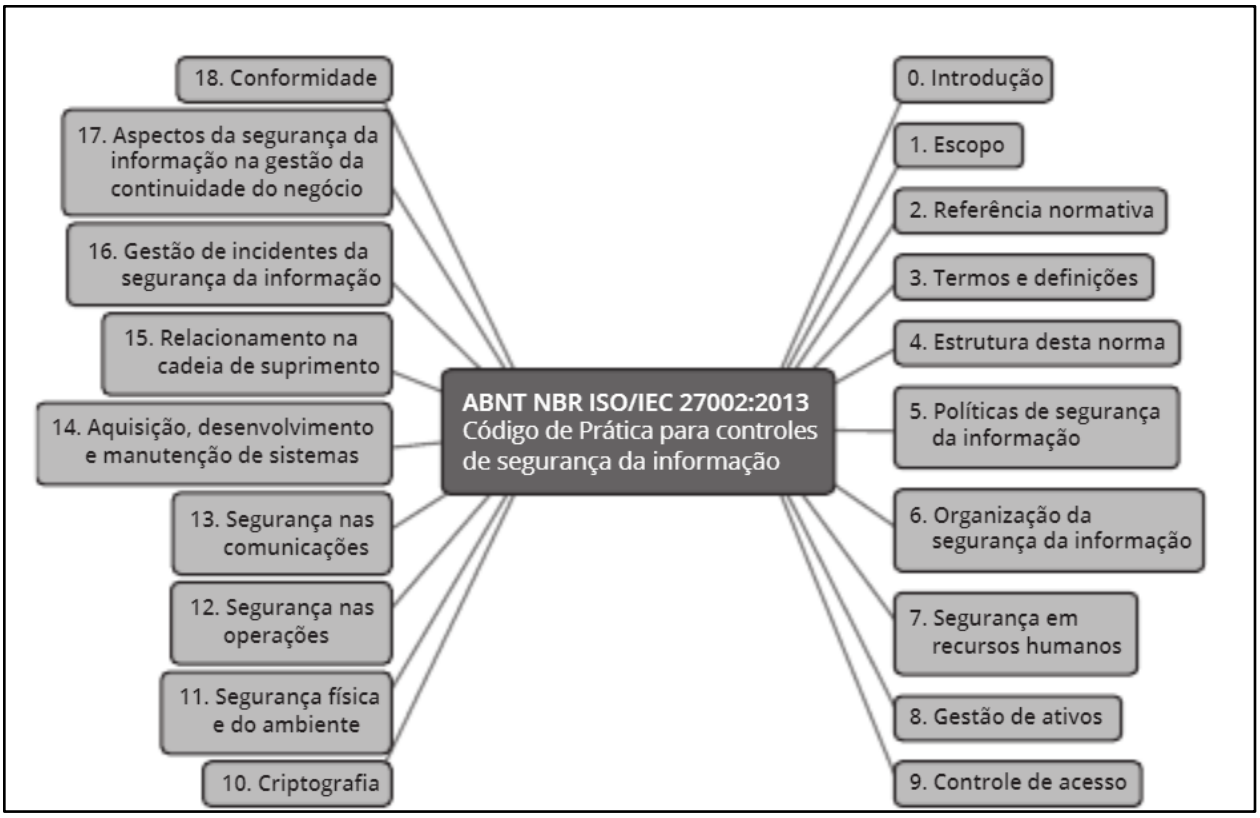

Figura 7: Esquema com todas as seções da norma ABNT NBR ISO IEC 27002:2013

Fonte: COELHO, ARAÚJO e BEZERRA (2014)

A Figura 7 ilustra todas as seções apresentadas na norma ABNT NBR ISO/IEC 27002:2013. Enquanto as seções 0 à 4 apresentam aspectos introdutórios da norma, as seções 5 à 18 apresentam os controles de segurança da informação.

Considerando o propósito deste projeto, a seção referente ao controle de Política de segurança da informação (quinto controle apresentado) será explicada com maior detalhamento neste trabalho. De acordo com a norma, esta seção tem como objetivo prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. A seção é subdividida em duas outras seções, conforme especifica COELHO, ARAÚJO e BEZERRA (2014, p. 21):

- Políticas para segurança da informação: Apresenta o que convém que o documento da política contenha, e a importância de que ela seja comunicada a todos os integrantes da organização. A seção aborda também exemplos de políticas específicas para apoiarem as políticas de segurança da informação.
- Análise crítica das políticas para segurança da informação: Apresenta como convém que seja realizada a análise crítica da política, pela direção da organização, em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Por fim, vale ressaltar, que mesmo que uma organização não tenha interesse em ser auditada e certificada na norma ISO 27001, seguir as boas práticas da ISO 27002 pode ajudá-la a alcançar um Sistema de Gestão de Segurança da Informação mais robusto.

3.6.3 Norma ABNT NBR ISO/IEC 27005:2011

Em 2011, a Associação Brasileira de Normas Técnicas (ABNT) realizou a publicação de mais uma norma para fazer parte da série de normas ISO/IEC 27000,

que foi chamada de ABNT NBR ISO/IEC 27005 - Tecnologia da Informação - Técnicas de Segurança - Gestão de riscos de segurança da informação.

A norma ABNT NBR ISO/IEC 27005:2011 define o processo de gestão de riscos como atividades coordenadas para dirigir e controlar os riscos de uma organização. Este processo pode ser dividido em seis processos, que são o de procedimento de definição do contexto, análise/avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco e monitoramento e análise crítica destes riscos. O processo de análise/avaliação de riscos pode ser subdividido em outras três etapas, que são a identificação de riscos, análise de riscos e avaliação de riscos. A organização e ordenação de cada um destes processos pode ser visualizado na Figura 8.

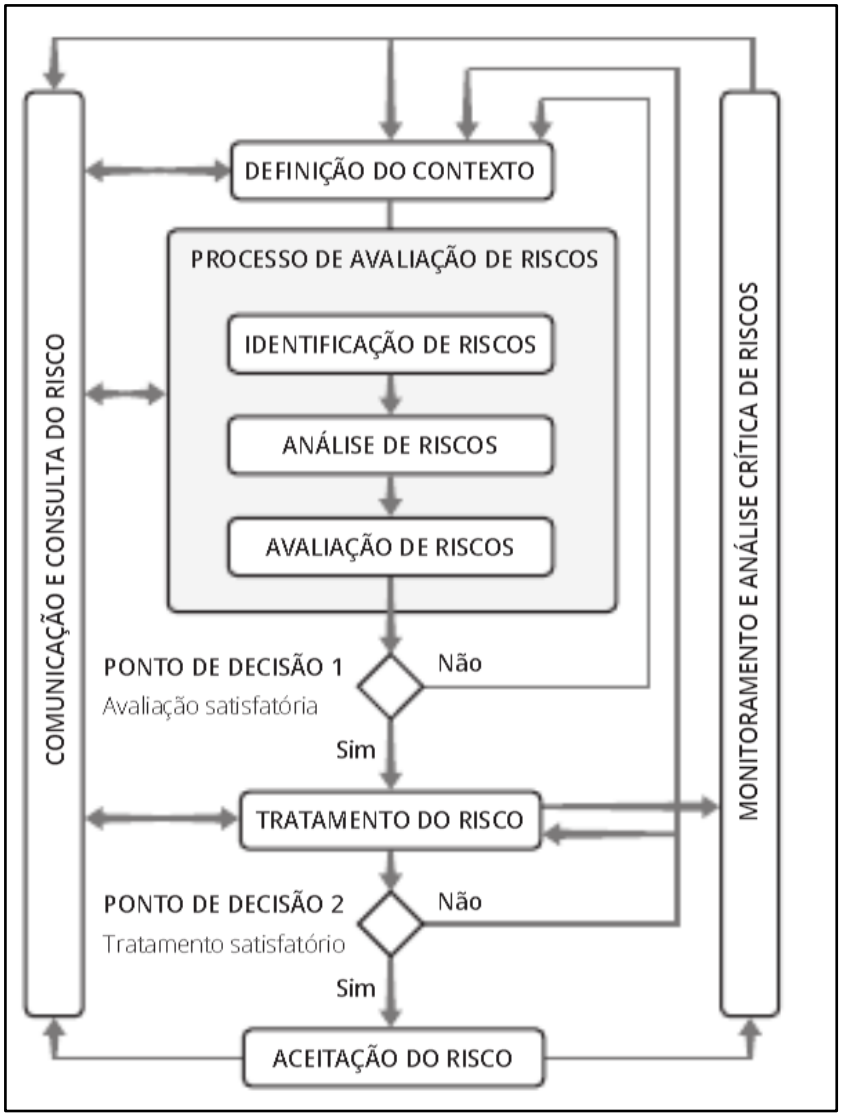

Figura 8: Processo de Gestão de Riscos
Fonte: ABNT NBR ISO 27005

Cada um destes passos pode ser definido da seguinte maneira (BEZERRA, 2013):

- Definição do contexto: Este passo é responsável pela definição do ambiente, escopo, critérios de avaliação, entre outras definições. Esta etapa é essencial para a equipe que realiza a gestão de risco conhecer todas as informações sobre a organização.
- Processo de avaliação de riscos: Este processo objetiva analisar os riscos em função dos impactos ao negócio e as probabilidades de sua ocorrência. Devem ser analisados todos os possíveis riscos, para que assim se saiba o quanto afetarão a organização, e determinar ações necessárias para reduzir estes riscos a um nível aceitável.
- Tratamento do risco: A partir dos resultados obtidos na análise e avaliação dos riscos, são definidos os controles necessários para o tratamento do risco. Para este passo, utiliza-se a norma ABNT NBR ISO/IEC 27002:2013, que especifica os controles que deverão ser implementados.
- Aceitação do risco: Este processo especifica os riscos que são aceitos pela organização, ou seja, os riscos que por algum motivo específico não serão tratados ou serão tratados parcialmente, conhecidos como riscos residuais.
- Monitoramento e análise crítica de riscos: Neste passo, é realizado o acompanhamento dos resultados, verificando se os processos aderidos estão tendo o retorno esperado. Desta forma, pode-se garantir a melhoria contínua do processo de gestão de riscos.
- Comunicação e consulta do risco: Neste processo, é realizado a comunicação do risco e da forma como será tratado, para todas as áreas operacionais e seus gestores. É uma etapa que deve ser executada em paralelo com todas as outras etapas do processo de gestão de riscos.

Os procedimentos especificados na norma são executados de maneira cíclica, na qual a gestão se desenvolve de maneira incremental, através de uma sucessão de iterações, e cada iteração libera uma entrega (saída) para a seguinte. Desta forma, se

aplicado os procedimentos da norma dentro de um processo PDCA , teremos o processo especificado pela Figura 9.

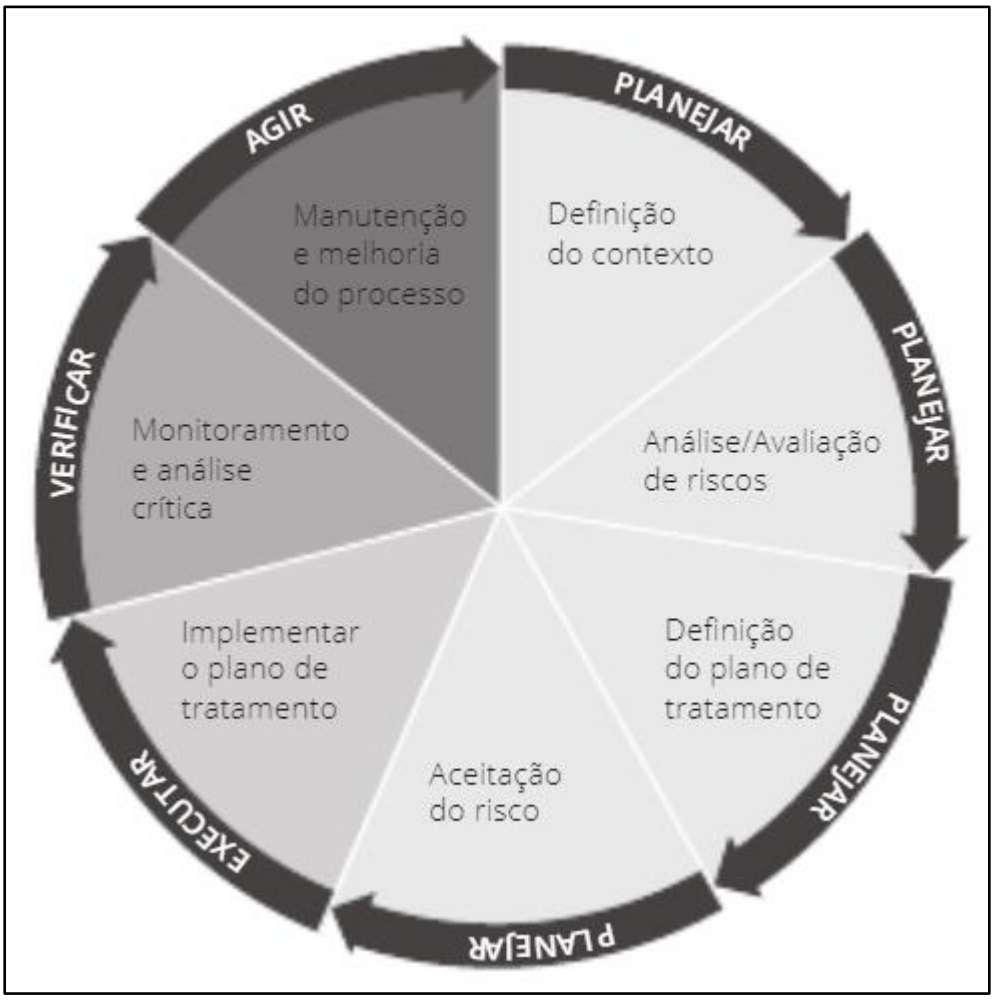

Figura 9: Aplicação dos passos da norma ABNT NBR ISO 27005:2011 no modelo PDCA
Fonte: BEZERRA (2013)

De acordo com a norma ABNT NBR ISO/IEC 27001, os controles implementados nos escopos, limites e contexto de um Sistema de Gestão de Segurança da Informação (SGSI) devem estar baseados no risco. E este requisito pode ser atendido através da aplicação do processo de gestão de riscos de segurança da informação (BEZERRA 2013). Desta forma, fica clara a relação complementar entre a norma ABNT NBR ISO/IEC 27001, ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005, quando se visa garantir a segurança da informação dentro de uma organização.

3.7 Política de Segurança da Informação (PSI)

Uma política de segurança da informação é definida por COELHO, ARAÚJO e BEZERRA (2014, p. 72).

> "A política de segurança da informação é um conjunto de diretrizes apoiado por normas e procedimentos, que determinam regras e práticas a serem seguidas, para assegurar a segurança da informação, conforme o ramo do negócio e requisitos legais, contratuais, regulamentares e normativos aplicáveis a todo o escopo da organização. Ela definirá as diretrizes, limites, as responsabilidades e os objetivos dos controles que deverão ser implementados e implantados para garantir os requisitos de proteção da segurança da informação na organização."

Desta forma, pode-se dizer que uma política de segurança mostra qual é a filosofia usada pela organização, visando assegurar que todas as suas informações e de seus clientes estejam protegidas de possíveis perdas, roubos ou outros danos.

Ainda, COELHO, ARAÚJO e BEZERRA (2014, p. 71) enfatizam que este conjunto de diretrizes devem ser especificadas em um documento, que pode ser considerado um documento jurídico. Este documento deve ser escrito de maneira clara, uma vez que seu conteúdo deve ser voltado para todos os membros da organização que, por sua vez, devem seguir as regras especificadas no mesmo.

SIMON 2008 e HARRIS 2013 definem que existem três tipos de PSI:

- Política segurança da informação organizacional: É uma política de alto nível, que visa definir a abordagem da organização em relação à segurança da informação. Este tipo de política define os objetivos do programa de segurança da informação da organização, bem como seus objetivos estratégicos e táticos para proteção da informação e ativos, além de abordar leis, regulamentações e responsabilidades relativas à questões de segurança da informação, e como elas devem ser satisfeitas, bem como questões de penalidades por descumprimento da política. A política de segurança organizacional fornece,

ainda, escopo e direção para todas as futuras atividades de segurança dentro da organização (SIMON 2008 e HARRIS 2013).

- Políticas de segurança de questões específicas: Este tipo de política foca em questões ou preocupações específicas, que a gerência sente necessidade de explicação mais detalhada e atenção, para garantir que uma estrutura abrangente seja construída e que todos os funcionários entendam qual a abordagem correta em relação ao que é tratado na política. Tem-se como exemplo deste tipo de documento: políticas sobre privacidade, uso de e-mail, uso apropriado de recursos do computador e gerenciamento de senhas (HARRIS 2013).

- Políticas de segurança específicas de sistemas: Aborda aspectos de segurança com relação à computadores, sistemas, redes e aplicativos. Esse tipo de política é direcionado para um ou um grupo de sistemas semelhantes e descreve como eles devem ser protegidos, ou seja, quem pode fazer o que a sistemas específicos e em que condições. Por exemplo, uma organização pode ter uma política descrevendo como um banco de dados contendo informações confidenciais deve ser protegido, quem pode ter acesso e como a auditoria deve ocorrer. Também pode ter uma política descrevendo como os laptops devem ser bloqueados e gerenciados (HARRIS 2013).

De maneira geral, qualquer um dos três tipos de PSI possuem as seguintes etapas de desenvolvimento (COELHO, ARAÚJO e BEZERRA 2014, p. 74):

- Identificar a legislação: Toda organização é submetida a diversas leis, normas, regulamentações, e estas devem ser cumpridas, a fim de que a organização não venha a sofrer com penalidades. Desta forma, é preciso levar em conta toda legislação que possa impactar no desenvolvimento da PSI.
- Identificar recursos críticos: É necessário realizar o levantamento dos recursos críticos da organização, ou seja, os recursos sob risco de

segurança. São incluídos nesta categoria recursos de hardware, software, dados, pessoas, documentação, suprimentos, etc.

- Analisar necessidades de segurança: Nesta etapa é realizada a análise de riscos, passo de extrema importância para o desenvolvimento de uma política de segurança adequada e, sendo assim, para a gestão da segurança da informação de uma organização. Nesta análise, procura-se identificar ameaças, impactos, componentes críticos, grau de proteção adequado, custos potenciais, entre outros aspectos.
- Elaborar proposta e promover discussão aberta: Neste ponto do processo, deve ser elaborada uma proposta de PSI, levando em conta os fatores estudados nos passos anteriores. Posteriormente, a proposta deve ser apresentada a todos os membros da organização envolvidos no processo de desenvolvimento da PSI.
- Apresentar documento: Após a apresentação e discussão da proposta inicial, a PSI deve ser documentada de maneira formal.
- Aprovar e implementar: Nesta fase, a documentação da política deve ser aprovada pelos dirigentes da organização. Com a aprovação, inicia-se a fase de implementação, onde devem ser executados todos os mecanismos de segurança definidos pela PSI desenvolvida, como soluções técnicas ou administrativas, por exemplo.
- Comunicar e treinar: Considerando que a segurança de uma organização envolve todos os seus membros, é de suma importância que, como parte da implementação da PSI, a mesma seja comunicada para toda a organização. É recomendado que esta apresentação faça parte de qualquer palestra, formação ou treinamento realizados à novos membros da organização.
- Manter a política de segurança: Uma PSI deve passar por análises periódicas, ou quando ocorrerem mudanças organizacionais significativas, como por exemplo incidentes de segurança ocorridos, ou ainda mudanças de tecnologias, legislação ou negócios. Estas análises visam manter a adequação e eficiência da PSI e, quando ocorrer alguma

> mudança, deve ser gerada uma nova documentação da PSI, que deve posteriormente ser novamente aprovada pelos dirigentes, bem como divulgada para a organização como um todo.

Quando em conformidade com normas ABNT NBR ISO/IEC 27002:2013, a PSI de um ambiente organizacional terá maior qualidade e confiabilidade, uma vez que esta norma foi desenvolvida para garantir os melhores resultados possíveis em manter a segurança da informação. Fica evidente, também, que no passo de elaboração da PSI de “Identificar recursos críticos”, a utilização da norma ABNT NBR ISO/IEC 27005:2011 pode servir de auxílio para os levantamentos necessário, de maneira eficaz e confiável.

3.8 Trabalhos correlatos

Com o propósito de fundamentar que a temática e a proposta abordada por este projeto mostra-se relevante, esta seção abordará alguns trabalhos correlatos que realizaram procedimentos e experimentos semelhantes ao proposto pelo presente trabalho.

3.8.1 Trabalho correlato 1: Políticas de Segurança da Informação: um estudo de caso baseado nas normas ABNT NRT ISO/IEC 27014:2013 e ABNT NRT ISO/IEC 27005:2011

ULLMANN (2015) realiza, neste trabalho, um estudo sobre a importância das políticas de segurança da informação, apresentando um resumo sobre as normas ABNT NBR ISO/IEC 27001:2006, ABNT NBR ISO/IEC 27002:2013, ABNT NBR ISO/IEC 27003:2011, ABNT NBR ISO/IEC 27004:2010, ABNT NBR ISO/IEC 27005:2011 e ABNT NBR ISO/IEC 27007:2012.

Com base no estudo desenvolvido, a autora realiza, então, um estudo de caso na empresa Soldas Rosense, que não utiliza nenhuma PSI, e utiliza medidas de segurança precárias. Inicialmente, a autora realiza o levantamento de informações sobre o ambiente a ser estudado, especificando equipamentos, estrutura física,

regulamentos e regras utilizadas pela empresa, e segue aplicando a gestão de risco conforme ABNT NBR ISO/IEC 27005:2011.

Como resultado do estudo, evidenciou-se diversos processos da organização que devem ser melhorados, como cabeamento de rede, instalação de câmeras de monitoramento, realocação do servidor, aquisição de HD externo, implantação de um sistema de refrigeramento para o servidor, implantação de um esquema mais seguro de senhas de acesso aos computadores, entre outros. Os pontos evidenciados no estudo foram então, aplicados em uma PSI, que passou a fazer parte da gestão de segurança da informação da mesma e será, posteriormente, gerenciada pelos membros da empresa.

3.8.2 Trabalho correlato 2: Desenvolvimento de uma Política de Segurança da Informação: Um caso de estudo (*Developing an Information Security Policy: A Case Study Approach*)

ALQAHTANI (2017) explorou, neste projeto, a implementação de uma PSI dentro de uma grande organização, para avaliar a adequação de políticas e para determinar a conscientização e conformidade do usuário com tais políticas. Através do estudo, evidenciou-se que as áreas de foco de segurança da informação incluídas nesta organização são o gerenciamento de senhas; uso de email, a Internet e sites de redes sociais; computação móvel; e manuseio de informações. Porém, os níveis de maturidade de segurança de cada área variavam, devido à falta de conhecimento e conformidade das PSI entre os usuários.

Foi evidenciado, através do estudos, que os responsáveis pela área de TI não estavam envolvidos com a PSI em vigor na empresa, uma vez que estes não haviam participado do desenvolvimento da PSI. A partir disto, ALQAHTANI (2017) concluiu que essa pode ser a principal razão para o baixo nível de maturidade de muitas das subáreas e alto nível em outras. A falta de participação dos gerentes no desenvolvimento das PSI antigas era provocada pela falta de motivação dos próprios gerentes, que não tratavam aspectos de segurança com a referida importância.

4. ESTUDO DE CASO: Elaboração de políticas de segurança em um ambiente de desenvolvimento

A partir dos conceitos apresentados na fundamentação teórica, será realizado um estudo de caso no laboratório Bridge, instituição que faz parte da Universidade Federal de Santa Catarina. Para evidenciar o perfil da instituição, algumas características iniciais podem ser descritas.

- É um laboratório de extensão da Universidade Federal de Santa Catarina.
- Está em atuação desde 2012.
- Atualmente conta com cerca de 115 membros, entre estes, gestores, desenvolvedores, *testers*, analistas, técnicos, entre outros.
- Realiza pesquisa e inovação em TI, através do desenvolvimento de soluções tecnológicas na área da saúde pública, vinculadas ao Ministério da Saúde e a ANVISA. Alguns dos projetos desenvolvidos incluem o e-SUS AB (Atenção Básica), o SISMOB (Sistema de Monitoramento de Obras), ambos do Ministério da Saúde e o RNI (Registro Nacional de Implantes) da ANVISA.
- Lida com dados sensíveis, uma vez que fazem uso de informações da área da saúde e do governo.
- Possui diversas medidas de segurança da informação aplicadas ao ambiente da instituição, mas carece de uma ou mais Políticas de Segurança da Informação formalmente desenvolvidas e documentadas.

Sendo assim, o estudo de caso fará o uso da norma ABNT NBR ISO/IEC 27005:2011 para realizar a gestão de riscos da instituição, realizando inicialmente a definição do contexto, processo de avaliação, tratamento e aceitação de riscos. Posteriormente serão aplicados os resultados deste processo no desenvolvimento de uma ou mais PSI que, de acordo com as normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013, prevê como passos a identificação da legislação, de recursos críticos, a elaboração e discussão da proposta com os membros responsáveis pelo laboratório, e posteriormente a apresentação e aprovação do documento. Quando

aprovada, as PSI passarão então pela fase de implementação, comunicação e alterações.

Espera-se que ao final do desenvolvimento deste projeto, seja gerado um ou mais documentos em conformidade com as normas utilizadas, e que estes tenham aplicabilidade efetiva para a instituição estudada, para que a mesma possa realizar a aplicação e futuras manutenções nas documentações geradas.

4.1 Metodologia

Para realizar o estudo de caso deste projeto, considerou-se aplicar o modelo PDCA (*Plan, Do, Act, Check*), recomendado pela ABNT NBR ISO/IEC 27001:2013. Ainda, foi considerado alocar dentro das etapas do PDCA, quando necessário e quando possível, cada uma das etapas para a elaboração de uma PSI, mencionadas por COELHO, ARAÚJO e BEZERRA (2014, p. 74). Esta alocação de etapas foi definida da seguinte maneira:

- Planejar (Plan): Definição de escopo, Identificar a legislação, identificar recursos críticos;
- Realizar (Do): Analisar necessidade de segurança, Elaborar a proposta, Apresentar documento, Aprovar e implementar;
- Checar (Check): Manter a política de segurança;
- Agir (act): Aplicar, se existirem, alterações necessárias levantadas na fase de Checar (Check).

4.1.1 Planejar (Plan)

Considerando a grande gama de possíveis PSI que podem ser desenvolvidas para uma instituição/organização/empresa e considerando o limite cronológico disposto para a elaboração deste projeto, inicialmente foi necessário estabelecer quais e quantas PSI poderiam ser desenvolvidas.

Tendo isto em vista, foram realizadas reuniões com membros do laboratório Bridge, nas quais ficou definido que a PSI organizacional deveria ser obrigatoriamente desenvolvida, por ser o tipo de política base e de mais alto nível entre todos os tipos de PSI.

Além disto, foi também realizado, juntamente com os membros da equipe, um levantamento de quais os tipos de ativos essenciais para o laboratório. Para isto, foi utilizada a lista de principais tipos de ativos, presente na ABNT NBR ISO/IEC 27001:2013 e adicionados no Anexo A. Com este levantamento, evidenciou-se que os ativos de informações possuem importância crítica para que o laboratório possa executar seus processos e alcançar seus objetivos. Desta forma, definiu-se que outras duas políticas deveriam ser desenvolvidas: Política de vazamento de informações e Política de proteção de informações.

A partir disto, evidenciou-se, através de demais encontros com a equipe de líderes do laboratório Bridge, que existe uma grande gama de informações que são gerenciadas pelo laboratório e, por este motivo, foi decidido que todas as políticas desenvolvidas deveriam limitar-se aos processos de Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge e Gestão e acesso às bases de dados de produção.

Com relação às possíveis legislações, evidenciou-se, através de reuniões com os membros do laboratório, que considerando o escopo das PSI, dos ativos e dos seus processos envolvidos, não existiam legislações específicas que deveriam ser incluídas ou consideradas ao desenvolver as PSI. Logo, esta etapa não resultou em conteúdo a ser incluído na PSI.

Com isto, finalizou-se a fase de Planejamento, uma vez que foram definidos o escopo, a legislação e os recursos críticos. A partir disto, iniciou-se a fase de Realizar (*Do*).

4.1.2 Realizar (Do)

Esta fase do projeto conta com a execução dos passos: Analisar necessidade de segurança, Elaborar a proposta, Apresentar documento, e Aprovar e implementar.

4.1.2.1 Analisar necessidade de segurança

A análise da necessidade de segurança compreende realizar a análise de riscos, abordada na norma ABNT NBR ISO/IEC 27005:2011, identificando as informações, sua classificação, e posteriormente avaliando ameaças, impactos, componentes críticos, grau de proteção adequado, entre outros aspectos. Para isto, os seguintes levantamentos foram realizados juntamente com os líderes do laboratório Bridge:

- Quais informações estão envolvidas nos processos de:
    - Gestão e acesso ao código fonte dos sistemas desenvolvidos pelo Bridge.
    - Gestão e acesso à base de dados de produção.

- Qual a classificação de cada informação

  Utilizou-se a classificação de WHITMAN e MATTORD (2011), ou seja:
    - Confidencial: Esta classificação engloba as informações mais sensíveis do laboratório, necessitando um controle mais restrito de acesso e manipulação das mesmas, que deve ser restrito a indivíduos e equipes específicas do ambiente;
    - Interna: Classificação utilizada para todas as informações que não se enquadram como Confidenciais, e podem ser acessadas apenas por membros internos do laboratório;
    - Externa: Toda informação que tenha sido aprovada pela gerência para divulgação pública.

- Realizar levantamento de riscos envolvendo cada uma das informações definidas anteriormente

  Foram identificados os seguintes riscos
    - Acesso não autorizado às informações, por agentes internos;
    - Acesso não autorizado às informações, por agentes externos;
    - Uso ou modificação não autorizada de informações, por agentes internos;

- Uso ou modificação não autorizada de informações, por agentes externos;
- Perda por circunstâncias ambientais (ex: fogo ou enchente);
- Roubo de equipamentos com armazenamento das informações;
- Roubo ou perda de informações por meio de transferência não autorizada (ex: utilização de mídias removíveis para transferência não autorizada das informações, ou transferência não autorizada em nuvem ou por outros métodos online);
- Falhas de sistema que acarretem no acesso ou modificação não autorizada das informações.

Cada um dos riscos foi avaliado para cada uma das informações levantadas, através do uso da matriz de risco apresentada na Tabela 2. Com isto, pode-se obter o grau de severidade que cada um dos riscos representa atualmente para o Bridge.

MATRIZ QUALITATIVA DE RISCOS		CONSEQUÊNCIA				
		Desprezível	Marginal	Médio	Crítico	Extremo
PROBABILIDADE	Quase certo					
	Provável					
	Possível					
	Pouco provável					
	Raro					

Intolerável Substancial Moderado Aceitável Trivial

Tabela 2: Matriz de risco

Fonte: Autora

- Realizar levantamentos de medidas de proteção que estão sendo aplicadas para evitar e mitigar a ocorrência dos riscos avaliados.

Com estes levantamentos feitos, foi possível partir para a próxima fase e iniciar a elaboração das PSI.

4.1.2.2 Elaborar a proposta

Com os resultados obtidos das fases anteriores, foi possível desenvolver todas as PSI planejadas, ou seja, a Política de Segurança da Informação Organizacional, contida no Anexo E, a Política de Proteção da Informação (Anexo F) e a Política de Vazamento de Informação (Anexo G). Todos os documentos foram divididos em seções, na qual algumas sessões são comuns entre todas as PSI e outras seções são exclusivas de cada PSI em específico.

Tem-se nas seções em comum entre todas as PSI desenvolvidas:

- Histórico de revisão
    - Considerando que uma PSI deve ser revisada periodicamente, este tópico auxilia a o laboratório Bridge a manter um controle sobre cada revisão realizada no documento. Para cada vez que o documento for revisado, deve ser incluído no Histórico de revisão: Versão, Data, Revisado por e Observações.

- Introdução
    - Este tópico serve para auxiliar a introduzir a PSI para o membro do laboratório, explicando qual a sua utilidade e importância em manter os aspectos de segurança da informação no Bridge.

- Propósito
    - Nesta seção é explicitado de maneira mais detalhada qual o propósito da presente PSI, e faz-se necessário uma vez que auxilia o membro a compreender o que a PSI deve cobrir e o que não irá cobrir.

- Escopo
    - Este tópico define para o membro do Bridge para qual escopo a PSI se aplica. São especificados os processos e ativos (pessoas, tecnologias, etc) incluídos neste escopo.

- Definições
    - Este tópico funciona como um glossário, onde os termos utilizados no decorrer da PSI são definidos, para auxiliar o entendimento de todo e qualquer membro que leia a PSI.

- Referências
    - Nesta seção são especificadas quaisquer referências utilizadas nas PSI, incluindo todas as ABNT ISO 27000 e outras políticas e demais materiais de segurança de informação do Bridge.

Dentre os tópicos exclusivos de cada PSI, estão os seguintes:

- PSI organizacional (Anexo E)
    - Cumprimento
        - Neste tópico é especificada a necessidade de cumprimento desta PSI e das outras PSI desenvolvidas pelo Bridge.

    - Papéis e Responsabilidades
        - Neste tópico são especificadas as responsabilidades gerais que os membros e o laboratório devem ter com a segurança da informação e de ativos:
            - Zelar pela segurança dos sistemas de informação, infraestrutura, aplicativos, produtos, serviços, redes de telecomunicações e demais recursos utilizados pelo laboratório Bridge, que auxiliam na criação, coleta, processamento, armazenamento, transmissão, análise e descarte de informações.
            - Siga e aplique as medidas especificadas na Política de Segurança da Informação Organizacional do Laboratório Bridge.

- Siga e aplique as medidas de proteção de dados especificados na Política de Proteção de Dados do Laboratório Bridge.
- Siga e aplique as medidas de vazamento de dados especificadas na Política de Vazamento de Dados do Laboratório Bridge.
- Garantir que todas as Políticas de Segurança da Informação do laboratório Bridge possuem livre acesso à todos os membros e colaboradores do laboratório.
- Garantir que todas as Políticas de Segurança da Informação do laboratório Bridge estão sendo devidamente aplicadas e seguidas por todos os colaboradores e membros do laboratório.
- Garantir que as Políticas de Segurança da Informação do laboratório Bridge sejam periodicamente revisadas e aprimoradas.
- Garantir a conformidade das Políticas de Segurança da Informação do Laboratório Bridge com as normas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISO/IEC 27005:2008.

- PSI de Proteção de Informação (Anexo F)
    - Tipos de Informações
        - Neste tópico são apresentadas todas as informações referentes aos processos na qual as PSI serão focadas. Foram evidenciados 7 tipos de informações que a PSI fará referência, que são:
            - Gestão e acesso ao código fonte dos sistemas desenvolvidos pelo Bridge
                - Código fonte do projeto SISMOB para plataforma web.

        - Código fonte do projeto SISMOB para plataforma mobile.
        - Código fonte do projeto e-SUS AB para plataforma web.
        - Código fonte do projeto e-SUS AB para plataforma mobile.
        - Código fonte do projeto RNI para plataforma web.
    - Gestão e acesso às bases de dados de produção
        - Gestão e acesso à base de dados de produção nacional.
        - Gestão e acesso à base de dados de produção municipal.

- Tipos de Incidentes
    - Nesta seção é evidenciado que incidentes, para a presente PSI, são riscos que afetam a confidencialidade, disponibilidade ou integridade das informações mencionadas no tópico de Tipos de Informações. Ao todo, foram evidenciados 8 tipos de incidentes na qual a PSI irá focar, que são:
        - Acesso não autorizado às informações confidenciais, por agentes internos.
        - Acesso não autorizado às informações internas, por agentes externos.
        - Uso ou modificação não autorizada às informações confidenciais, por agentes internos.
        - Uso ou modificação não autorizada às informações internas, por agentes externos.
        - Perda por circunstâncias ambientais (ex: fogo ou enchente).
        - Roubo de equipamentos do Bridge com armazenamento de informações.

- Roubo ou perda de informações por meio de transferência não autorizada (ex: utilização de mídias removíveis para transferência não autorizada das informações, ou transferência não autorizada em nuvem ou por outros métodos online).
- Falhas de sistema que acarretem no acesso ou modificação não autorizada das informações.

- Medidas de proteção
  - Nesta última seção da PSI, são apresentadas todas as medidas que os membros do laboratório Bridge devem seguir e aplicar para proteger as informações especificadas no tópico de Tipos de Informações, dos riscos especificados no tópico de Tipos de Incidentes. Ao todo, foram especificadas 18 medidas de proteção:
    - Todo membro do laboratório deve utilizar senha de bloqueio para seus respectivos terminais de trabalho.
    - Todo colaborador deve manter a senha de acesso ao seu terminal de trabalho em sigilo.
    - Todo membro do laboratório deve manter em sigilo a sua senha de acesso aos repositórios da plataforma Google Drive do laboratório Bridge.
    - Todo membro do laboratório Bridge, que possuir acesso aos repositórios da plataforma Google Drive do Bridge, não deve realizar o compartilhamento de conteúdo com membros externos do laboratório Bridge.
    - Todo membro do laboratório Bridge, que possuir acesso aos repositórios da plataforma Google Drive do Bridge não deve conceder acesso ao repositório para membros externos do laboratório Bridge.
    - Todo membro do laboratório Bridge, que possuir acesso aos repositórios de código fonte de projetos do Bridge através

do GitHub, deve manter em sigilo o acesso ao mesmo, não divulgando os códigos (parcial ou totalmente) para membros não autorizados.

- Todo membro do laboratório Bridge, que possuir acesso aos repositórios de código fonte de projetos do Bridge através do GitHub não deve realizar cópia ou modificação não autorizada no código (parcial ou totalmente).
- Todo membro do laboratório Bridge deve assinar e seguir pontualmente todas as solicitações especificadas no Termo de Confidencialidade do laboratório Bridge.
- Qualquer colaborador que realizar o acesso ou utilização de informações do banco de dados produção (nacional ou municipal), através do seu terminal de trabalho, deve prontamente excluir estas informações do seu terminal após finalizada a sua utilização.
- Deve ser mantido controle de acesso aos ambientes do laboratório Bridge através de cartão magnético exclusivo do laboratório Bridge.
- Deve ser mantido o monitoramento contínuo de ambientes do laboratório Bridge através de câmeras de vigilância.
- Todo código de projeto deve possuir cópia de segurança (backup) nos servidores do laboratório Bridge.
- O colaborador que deixar de possuir vínculo com o laboratório Bridge deve prontamente ter seu acesso desligado dos seguintes serviços
    - Repositórios na plataforma Google Drive do laboratório Bridge.
    - RedMine do projeto e-SUS AB.
    - RedMine do projeto SISMOB.
    - Repositório do Bridge na plataforma GitHub.

- Deve ser mantido o acesso aos repositórios de código na plataforma GitHub apenas para os membros internos do Laboratório Bridge.
- Deve ser mantido o acesso aos repositórios na plataforma Google Drive do laboratório Bridge apenas para os membros internos do Laboratório Bridge.
- Repositórios na plataforma Google Drive do laboratório Bridge, que sejam confidenciais, devem ter seu acesso restrito apenas para membros ou equipes específicas.
- Deve ser solicitado autenticação em dois passos para os donos (*owners*) dos repositórios de código na plataforma GitHub.
- Ao realizar repasse, descarte ou substituição de terminais de trabalho (parcial ou totalmente), deve ser realizada a formatação do mesmo, a fim de apagar eventuais informações confidenciais ou internas que possam estar armazenadas.

- PSI de Vazamento de Informação (Anexo G)
    - Classificação das Informações
        - Nesta seção foi realizada a classificação das informações na qual a PSI é focada. Foi utilizada, como mencionado, a classificação de WHITMAN e MATTORD (2011): Interna, Externa e Confidencial.
            - Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge
                - Código fonte do projeto SISMOB para plataforma web - Nível Interno.
                - Código fonte do projeto SISMOB para plataforma mobile - Nível Interno.
                - Código fonte do projeto e-SUS AB para plataforma web - Nível Interno.

        - Código fonte do projeto e-SUS AB para plataforma mobile - Nível Interno.
        - Código fonte do projeto RNI para plataforma web - Nível Interno.
    - Gestão e acesso às bases de dados de produção
        - Gestão e acesso à base de dados de produção nacional - Nível Confidencial.
        - Gestão e acesso à base de dados de produção municipal - Nível Confidencial.

- Incidentes de Vazamento de Informações
    - Neste tópico é explicado quais tipos de incidentes podem ser classificados como incidente de vazamento de dados. Majoritariamente, estes incidentes são os mesmos evidenciados no tópico de Tipo de Incidentes, na PSI de Proteção de Informação.
        - Acesso não autorizado às informações confidenciais, por agentes internos.
        - Acesso não autorizado às informações internas, por agentes externos.
        - Uso ou modificação não autorizada das informações confidenciais, por agentes internos.
        - Uso ou modificação não autorizada das informações internas, por agentes externos.
        - Roubo de equipamentos do Bridge com armazenamento de informações.
        - Roubo ou perda de informações por meio de transferência não autorizada (ex: utilização de mídias removíveis para transferência não autorizada das informações, ou transferência não autorizada em nuvem ou por outros métodos online).

- Falhas de sistema que acarretem no acesso ou modificação não autorizada das informações.

- Plano de comunicação de Vazamento de Informações
  - Este tópico explora como deve ser tratado um incidente de vazamento de informação. É dividido em duas partes:
    - Comunicar vazamento: Especifica quais diretrizes devem ser seguidas por um membro do Bridge que identifique um incidente de vazamento de informação. Nesta parte é apresentado um formulário de comunicação de vazamento, presente no Anexo B.
    - Avaliação e Resposta: Nesta parte é explicado como a equipe responsável resolverá um incidente de vazamento de dados, orientando através das regras abaixo as medidas a serem tomadas.
      - Tipo de informação(ões) envolvida(s) no vazamento e sua(s) sensibilidade(s).
      - As medidas de proteção em vigor, que estão relacionadas com a(s) informação(ões) vazada(s);
      - O que aconteceu com a informação (por exemplo, foi perdida ou roubada).
      - Quantidade de pessoas envolvidas no vazamento, e quem são estas pessoas.
      - Se há consequências mais amplas para a vazamento.
      - Onde e como os as informações referentes ao vazamento são mantidas e como são armazenadas.
      - Uma vez que o incidente inicial esteja contido, deve ser realizado uma revisão completa das causas do vazamento e a eficácia da(s) resposta(s).

- Onde estão os maiores riscos, incluindo a identificação de possíveis pontos fracos dentro das medidas de segurança existentes.
- Deve ser realizada uma revisão nos sistemas, políticas, procedimentos e demais controles existentes, a fim de determinar sua adequação com a realidade do laboratório Bridge.
- Revisado os pontos anteriores, deve(m) ser aplicada(s) eventuais mudanças nos controles existentes, adaptando-o para as necessidades atuais.
- Avaliar a necessidade de conscientização de demais membros do laboratório Bridge acerca do vazamento ou de possíveis mudanças em políticas ou demais procedimentos de segurança.
- Ao finalizar a avaliação e investigação de todos os itens anteriores, deve ser realizado o preenchimento do “Formulário resposta de incidente de vazamento de informação do laboratório Bridge”, contido nos Anexos deste documento.

Juntamente com este tópico, é apresentado um formulário de resposta a incidentes de vazamento de informação, presente nos Anexos.

4.1.2.3 Apresentar documento, aprovar e implementar

A última etapa da fase de Realizar conta com a apresentação, aprovação e implementação dos documentos. Após finalizada todas as documentações das PSI, as mesmas foram apresentadas e repassadas para os membros responsáveis em aprovar as PSI. Após aprovadas, seguiu-se para a fase de implementação da PSI, na qual as mesmas foram repassadas para todos os membros da equipe de líderes do laboratório Bridge.

A partir da apresentação, aprovação e implementação, pode ser iniciada as últimas fases do PDCA do desenvolvimento das PSI.

4.1.3 Checar (*Check*)

Esta fase do PDCA consiste em fazer o controle das PSI, verificando a necessidade de possíveis mudanças a serem realizadas nas mesmas.

Para realizar essa verificação, foi aplicado para a equipe de líderes do Bridge um questionário de *feedback* referente às PSI, apresentado no Anexo D. O questionário consistiu em aplicar perguntas que auxiliassem a verificar a aceitabilidade, entendimento e coerência das PSI, por parte dos membros do laboratório.

1. Você tinha conhecimento sobre o que era uma política de segurança da informação, antes de ter conhecimento das PSI do Bridge?

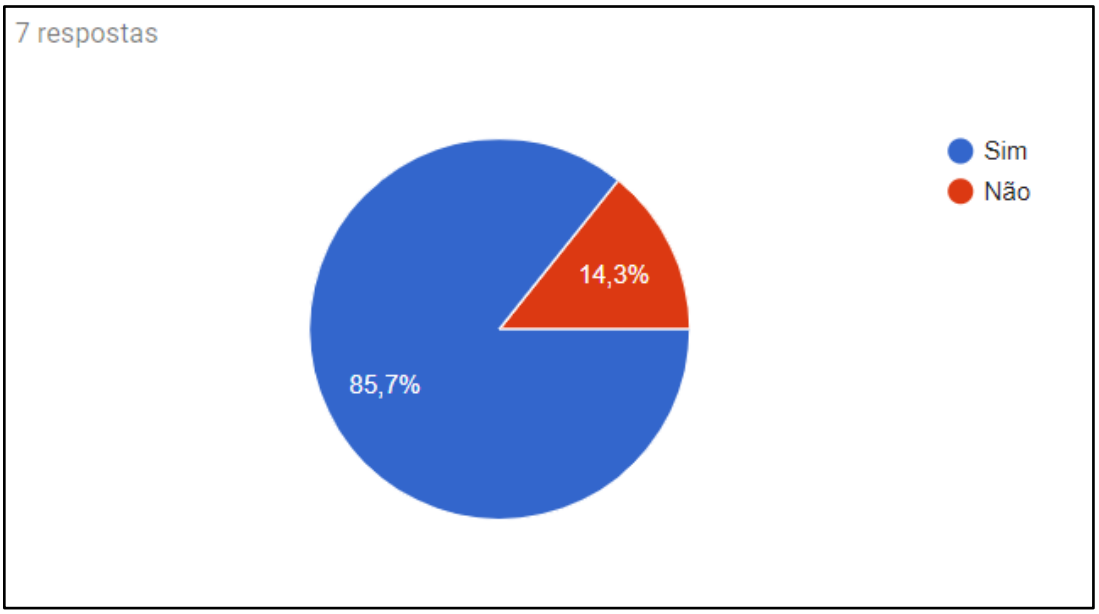

Figura 10: Questão 1 do questionário de feedback das PSI do Bridge

Fonte: Autora

Com esta pergunta foi possível verificar se os membros já possuíam conhecimento da técnica de PSI, antes da aplicação da mesma no Bridge.

Verifica-se que a grande maioria já tinha conhecimento da técnica (85,7%), o que representa algo positivo, embora este conhecimento não tenha sido posto em prática até então pelo laboratório. Em 14,3% das respostas, não havia conhecimento prévio da técnica de PSI, o que representa que o desenvolvimento e a aplicação das PSI do Bridge levou para estes membros o conhecimento desta técnica de segurança da informação.

2. Achou as políticas desenvolvidas pelo Bridge compreensíveis e de fácil entendimento?

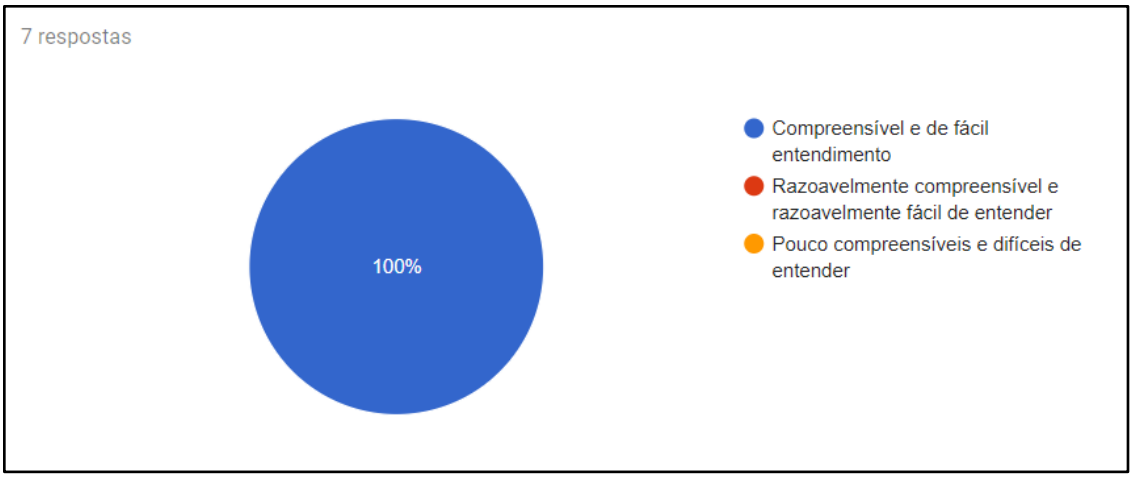

Figura 11: Questão 2 do questionário de feedback das PSI do Bridge

Fonte: Autora

Esta pergunta serve para evidenciar a clareza com que as PSI foram elaboradas, uma vez que as mesmas precisam ser de fácil entendimento para qualquer leitor, para que a mesma possa ser colocada em vigor por cada colaborador. Possuir um resultado unânime de respostas “Compreensível e de fácil entendimento” demonstra um resultado positivo neste quesito de clareza das PSI.

3. A partir do que foi especificado na PSI de Vazamento de Informações, você acredita que é capaz de identificar um vazamento de informação?

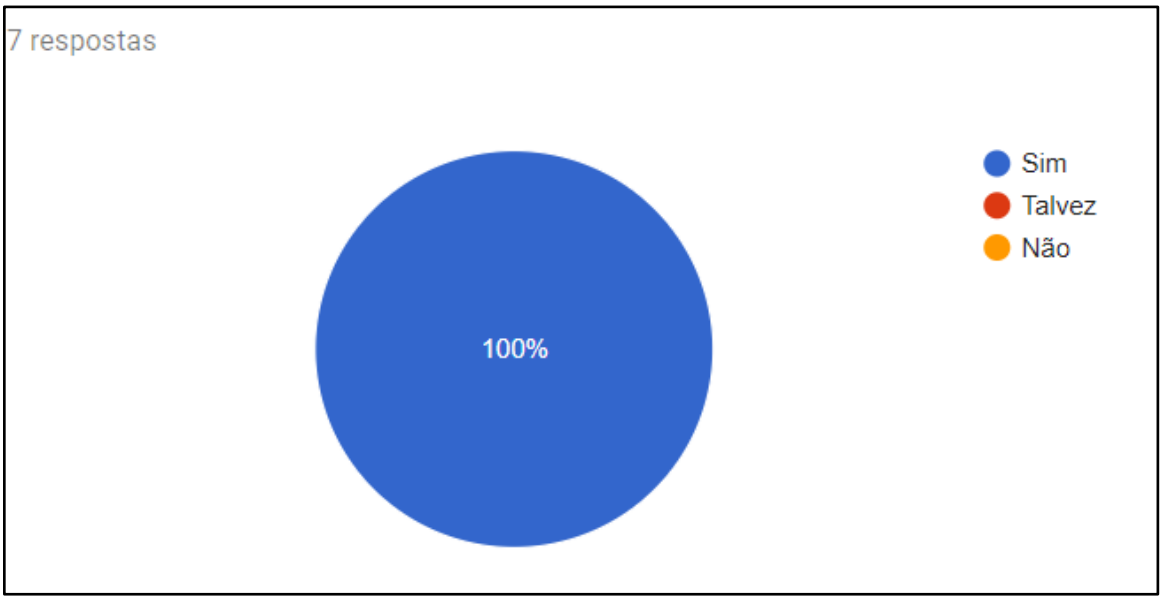

Figura 12: Questão 3 do questionário de feedback das PSI do Bridge

Fonte: Autora

Esta pergunta auxilia o Bridge a compreender se a PSI de Vazamento de Informações conseguirá atingir um de seus principais objetivos, que é o membro conseguir identificar o vazamento de informações. Novamente, a unanimidade de respostas “Sim” evidencia um resultado positivo para este quesito.

4. A partir do que foi especificado na PSI de Vazamento de Informações, você acredita que é capaz de reportar um vazamento de informação?

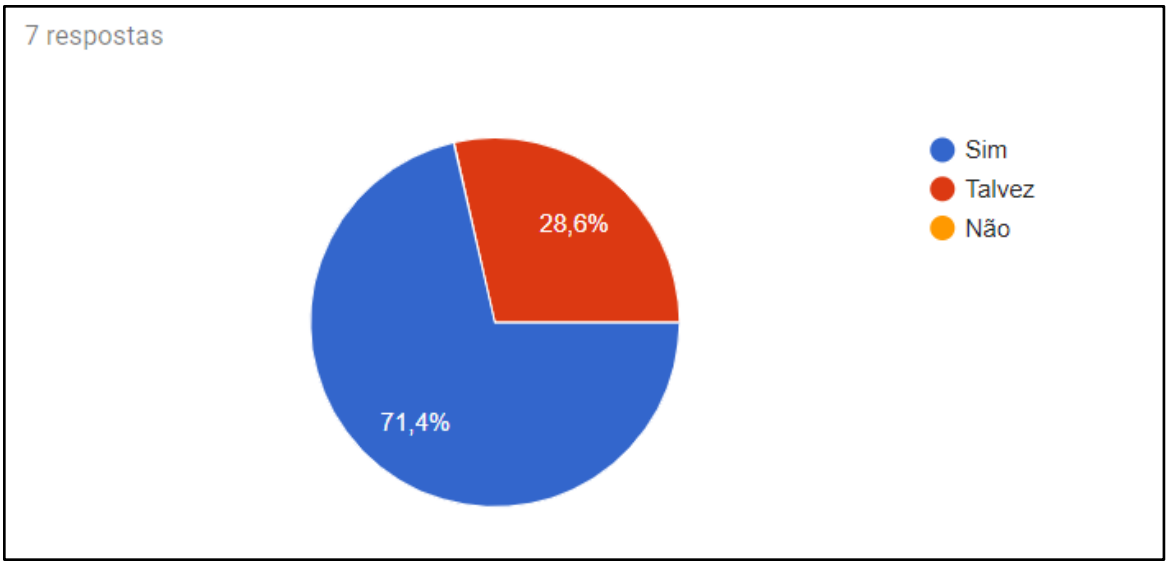

Figura 13: Questão 4 do questionário de feedback das PSI do Bridge

Fonte: Autora

Assim como a pergunta 3, esta pergunta auxilia o Bridge a compreender se a PSI de Vazamento de Informações conseguirá atingir outro de seus principais objetivos, que é o membro conseguir reportar um vazamento de informações. O fato de 28,6% das respostas terem sido “Talvez” evidencia que este quesito necessita ser futuramente analisado e melhorado na PSI.

5. A partir do que foi especificado na PSI de Proteção de Informações, você consegue compreender quais tipos de informações e tipos de incidentes a PSI está tentando proteger?

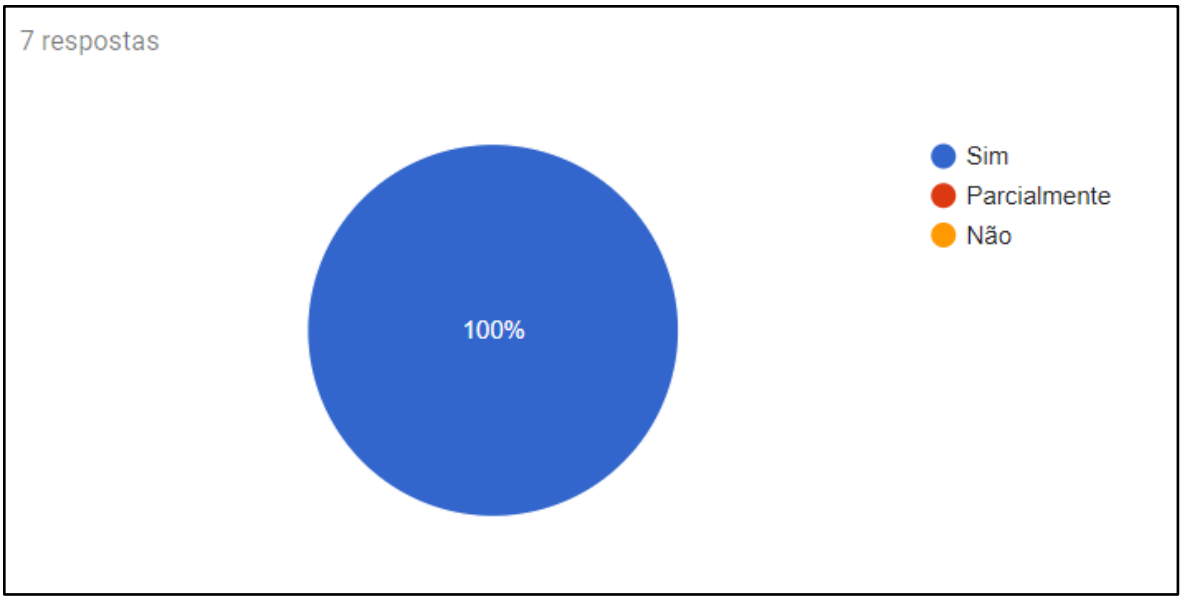

Figura 14: Questão 5 do questionário de feedback das PSI do Bridge

Fonte: Autora

Esta pergunta auxilia o Bridge a compreender se a PSI de Proteção de Informações conseguirá atingir um de seus principais objetivos, que é o membro conseguir identificar os tipos de informações que a PSI faz referência. Novamente, a unanimidade de respostas “Sim” evidencia um resultado positivo para este quesito.

6. A partir do que foi especificado na PSI de Proteção de Informações, você consegue compreender as medidas de proteção aplicadas pelo Bridge?

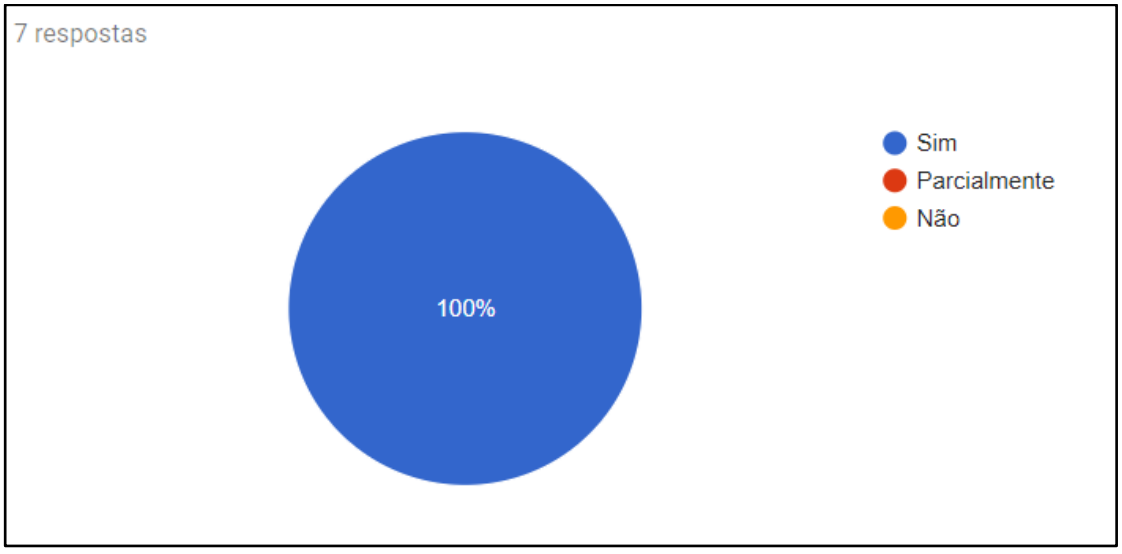

Figura 15: Questão 6 do questionário de feedback das PSI do Bridge

Fonte: Autora

Esta pergunta, assim como a pergunta 5, auxilia o Bridge a compreender se a PSI de Proteção de Informações conseguirá atingir outro de seus principais objetivos, que é o membro conseguir compreender as medidas de proteção especificadas na PSI, que devem ser seguidas e aplicadas. Também, assim como a pergunta 5, a unanimidade de respostas “Sim” evidencia um resultado positivo para este quesito.

7. A partir do que foi especificado na PSI de Proteção de Informações, você identifica alguma medida de proteção especificada na PSI que você ainda não está aplicando?

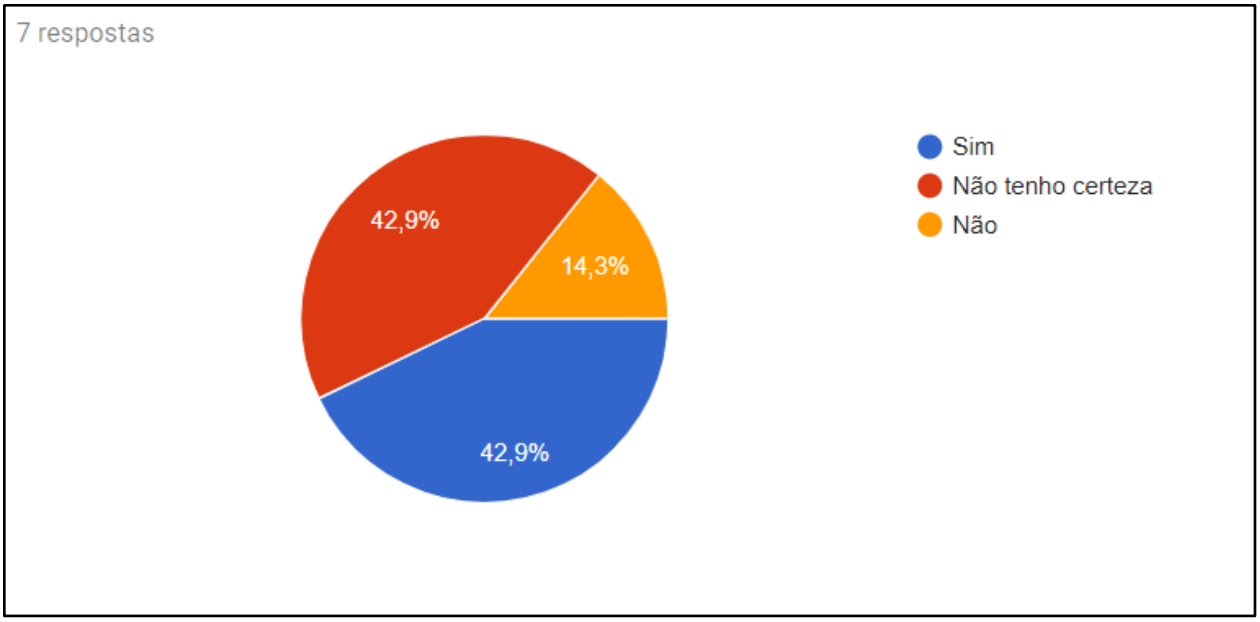

Figura 16: Questão 7 do questionário de feedback das PSI do Bridge

Fonte: Autora

Esta questão serve para evidenciar a eficácia da PSI de Proteção de Informação no ambiente Bridge. Evidencia-se, dentre as respostas de incerteza (42,9%), a necessidade de verificar com os membros se esta resposta se deve ao fato da medida não estar especificada o suficiente para que o mesmo pudesse dar uma resposta positiva ou negativa. Ainda, tanto para os membros

que responderam positivamente, quanto aos que responderam com incerteza, totalizando 57,2%, deve ser realizada uma análise e uma fiscalização futura para verificar se as medidas passarão a ser aplicadas por estes membros.

8. Concorda que as políticas auxiliam a garantir a segurança das informações no laboratório Bridge?

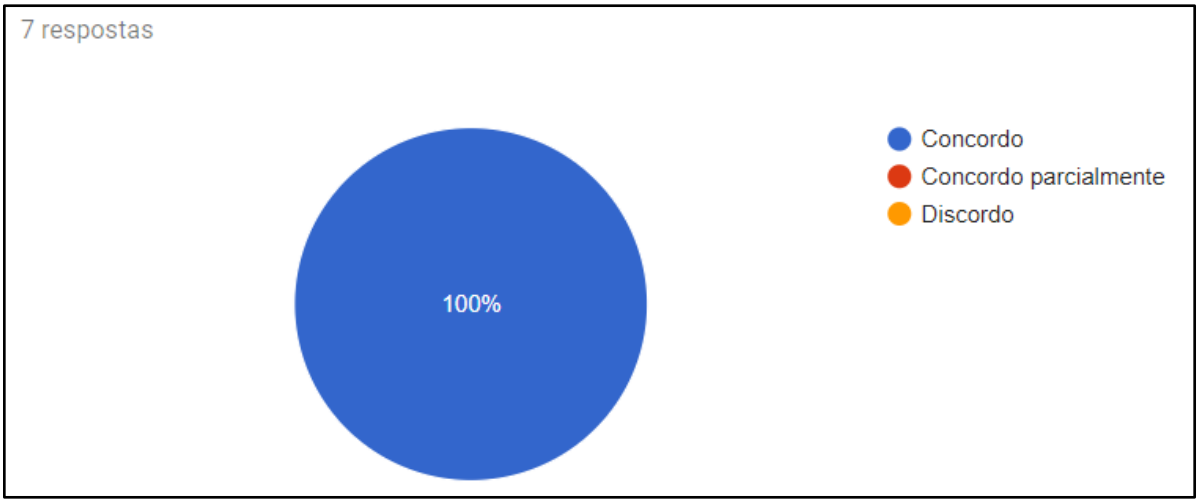

Figura 17: Questão 8 do questionário de feedback das PSI do Bridge

Fonte: Autora

Por fim, esta questão ajuda a entender se o leitor, após ler as três PSI desenvolvidas, consegue compreender a importância das mesmas para auxiliar a garantir a segurança da informação no Bridge. A unanimidade de respostas “Sim” evidencia um resultado positivo para este quesito.

Ainda, com o questionário foi possível realizar um levantamento de possíveis alterações a serem realizadas, abrindo um espaço para que o membro pudesse deixar opiniões, críticas e sugestões de melhoria para as PSI desenvolvidas. Foram utilizadas as seguintes perguntas, com um texto de livre digitação:

1. Tem alguma sugestão de melhoria futura para as políticas desenvolvidas?
2. Possui alguma outra observação em relação às PSI?

Através das respostas obtidas pelo questionário de *feedback* (Anexo D), podem ser levantadas as seguintes alterações:

1. Alterações de nomenclatura nos nomes de um dos processos.
2. Maior detalhamento das diretrizes a serem seguidas pela equipe responsável em gerenciar o vazamento, contido no tópico Avaliação e Resposta, da PSI de Vazamento de Informações do Bridge.
3. Retirada de uma das regras contidas no tópico de Medidas de Proteção da PSI de Proteção de Informações do Bridge, uma vez que a medida não será mais aplicada.
4. Substituição do Formulário para reportar incidente de vazamento de informação no laboratório Bridge (Anexo B) e do Formulário de resposta de incidente de vazamento de informação do laboratório Bridge (Anexo C) por versões *online*, possibilitando ao usuário reportar vazamento de maneira anônima.

4.1.4 Agir (*Act*)

Esta é a fase final do PDCA, e consiste em realizar as possíveis mudanças levantadas na etapa anterior, Checar (Check).

Considerando questões de recursos, cronologia e adequação ao PDCA, as alterações contidas no item 1, do tópico de Checar (Check) são consideradas viáveis para serem aplicadas para na fase de Agir (Act), para a versão 1.0 das PSI, enquanto as alterações dos itens 2, 3 e 4 devem ser consideradas nas próximas execuções do PDCA e incluídas em versões posteriores das PSI.

4.1.5 Conformidade com as normas

Ao finalizar as adaptações possíveis dentro da etapa de Agir (Act), considera-se o desenvolvimento das PSI finalizados neste primeiro ciclo de PDCA.

Em uma avaliação final no desenvolvimento das PSI, observou-se que foi possível manter a conformidade com as normas especificadas nos objetivos deste trabalho. Esta conformidade se mostrou presente da seguinte maneira:

- ABNT NBR ISO/IEC 27001:2013: Assim como determinado na norma, um SGSI deve ser implementado utilizando a estratégia PDCA. Esta estratégia foi aplicada para realizar o desenvolvimento de todas as PSI determinadas e, desta forma, está de acordo com esta norma.
- ABNT NBR ISO/IEC 27002:2013: Esta norma estabelece diversos controles que auxiliam a melhorar a qualidade do SGSI. Dentre os 11 controles estabelecidos na norma, foi possível aplicar os seguintes controles e subcontroles ao desenvolver as PSI
    - Políticas de Segurança da informação
        - Políticas de Segurança da Informação: Considera-se este controle aplicado, uma vez que, assim como estabelecido na norma, foi desenvolvido um conjunto de políticas de segurança de informação, que posteriormente foram aprovadas e comunicadas aos membros do laboratório;
    - Organização da segurança da informação
        - Responsabilidades e papéis pela segurança da informação - Considerando que as responsabilidades pela segurança da informação foram definidas e atribuídas, como consta na PSI Organizacional, no tópico de papéis e responsabilidades e na PSI de Proteção de Informação, no tópico de Medidas de proteção, pode-se concluir que este controle foi aplicado;
        - Contato com autoridades: Este controle foi aplicado uma vez que foram estabelecidos os grupos que responderão aos incidentes de vazamento de dados, e os grupos responsáveis pela revisão das políticas, como consta na PSI de Vazamento de Informação;
    - Gestão de ativos
        - Classificação da informação: Considera-se este controle aplicado, pois assim como é estabelecido na norma, um SGSI necessita assegurar que a informação receba um nível adequado de proteção, de acordo com a sua

importância na organização, e este processo foi realizado durante o desenvolvimento das PSI, no passo de Realizar (*Do*);

- Controle de acesso
  - Controle de acesso ao sistema e à aplicação: Este controle estabelece que deve ser realizada a prevenção ao acesso não autorizado aos sistemas e aplicações, que foi um dos riscos abordados ao desenvolver as PSI, e devidamente tratado através de controle de acesso ao código fonte de programas, procedimentos seguros de entrada no sistema e restrição de acesso à informação, especificado no tópico de Medidas de Proteção, na PSI de Proteção da Informação;

- ABNT NBR ISO/IEC 27005:2011: Esta norma estabelece a gestão de riscos em uma organização, abordagem que foi seguida durante o desenvolvimento das PSI, na qual foi devidamente aplicada no passo de Análise da necessidade da segurança, na etapa de Realizar (*Do*).

5. CONSIDERAÇÕES FINAIS

5.1 Conclusão

Na etapa inicial do projeto, foram levantados aspectos relevantes que envolvem o estudo de caso proposto. Foram abordados conceitos de classificação da informação, características da informação, segurança da informação, riscos, vulnerabilidades, ameaças e ataques, técnicas de defesa, normas e políticas de segurança da informação. Os tópicos abordados nesta fase serviram de embasamento teórico para a etapa seguinte do projeto.

Na fase final do projeto, foi realizado o desenvolvimento de três políticas de segurança da informação, uma PSI organizacional, uma PSI de Proteção de Informação e uma PSI de Vazamento de Informação. O desenvolvimento destas políticas foi dividido dentro do processo de PDCA, como requisitado pela norma ABNT NBR ISO/IEC 27001:2013. Inicialmente, as fases de Planejar (*Plan*) e Realizar (*Do*), envolveram uma série de reuniões com diversos membros do laboratório Bridge, a fim de realizar todos os levantamentos e avaliações necessárias para a elaboração das PSI. Posteriormente, com as PSI já finalizadas, foram realizadas a aprovação e na sequência a implementação das mesmas, que consistiu em divulgar as PSI e coletar um feedback sobre as mesmas. Com o feedback, foram realizadas as duas fases finais de Checar (*Check*) e Agir (*Act*), que consistiu em avaliar a necessidade de mudanças nas PSI e aplicar tais mudanças.

Considera-se que o presente projeto tenha sido um sucesso, uma vez que foi possível concluir o desenvolvimento prático das PSI e este desenvolvimento possuiu uma boa sinergia com os estudos teóricos realizados, abrangendo e utilizando as terminologias, conceitos, técnicas e todas as normas ABNT ISO mencionadas. Ainda, a elaboração das PSI trouxe ganhos para o laboratório Bridge, não apenas com as documentações como produto final, mas também no fato de que seu desenvolvimento auxiliou os membros do ambiente a pensar e avaliar com um maior foco e interesse às questões de segurança da informação no Bridge, envolvendo ativos, vulnerabilidades, riscos, medidas de proteção, entre outros aspectos.

5.2 Trabalhos futuros

Inicialmente, um próximo passo para a versão 1.0 das PSI elaboradas seria iniciar a expansão da aplicação da PSI para o resto dos membros do laboratório, aplicando o questionário de feedback para os mesmos, e coletando um maior número de sugestões de melhorias.

Ainda, uma vez que o processo PDCA é cíclico, e que PSI devem ser revisadas e melhoradas periodicamente, uma melhoria futura seria realizar a inclusão incremental de outros processos no escopo das PSI, realizando todo o processo de PDCA a medida que um novo processo for incluído na documentação. Desta forma, gradativamente as PSI poderão garantir a confidencialidade, disponibilidade e integridade do máximo de informações possíveis

Por fim, outra abordagem que deve ser considerada é uma futura reavaliação de ativos, semelhante a avaliação que foi realizada na fase de Planejamento (*Plan*). Desta forma, pode ser considerada a necessidade do desenvolvimento de PSI voltadas para outros ativos, como ativos de hardware, software, ou pessoas. Esta abordagem auxiliaria o Bridge a expandir medidas de seguranças em outras áreas, além dos ativos de informação, trazendo uma maior segurança para o ambiente.

REFERÊNCIAS

ALQAHTANI, F. H. Developing an Information Security Policy: A Case Study Approach. 4th Information Systems International Conference 2017, ISICO 2017, Novembro 2017, Bali, Indonesia.

ALSHAMMARI, M.; BACH, C. Defense Mechanisms for Computer-Based Information Systems. International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. PROJETO ABNT NBR ISO/IEC 27002:2013 - Código de Prática para controles de segurança da informação. Setembro de 2013.

BEZERRA, E. K. Gestão de Riscos de TI: NBR 27005. Rede Nacional de Ensino e Pesquisa. 2013.

CALDER, A. Nine Steps to Success: An ISO 27001 Implementation Overview, North American edition**.** 1. ed. 2016. p. 63-64

CATEGORY: vulnerability. Disponível em: <https://www.owasp.org/index.php/Category:Vulnerability> . Acesso em 09 de janeiro de 2018.

Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil. Estatísticas dos Incidentes Reportados ao CERT.br Por Ano. 2016. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em 07 de janeiro de 2018.

COELHO, F. E. S.; ARAÚJO, L. G. S.; BEZERRA, E. K. Gestão de Segurança da Informação: NBR 27001 e NBR 27002. Rede Nacional de Ensino e Pesquisa. 2014.

DARYUS Strategic Risk Consulting. Pesquisa Nacional de Segurança da Informação 2014: Uma visão estratégica dos principais elementos da Segurança da Informação no Brasil. 2014.

DIAS, C. Segurança e Auditoria da Tecnologia da Informação. Axcel Books. Rio de Janeiro, 2000.

DISTERER, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security. p. 92-100. 2013.

EY. 19ª Pesquisa Global de Segurança da Informação. 2017.

HARRIS, S. “All in One - CISSP Exam Guide”. 6 ed. 2013

HUMPHREYS, T. **“**State-of-the-art information security management systems with ISO/IEC 27001:2005”**.** ISO Management Systems. p. 15-16. Janeiro - Fevereiro 2006.

International Organization for Standardization. The main benefits of ISO standards. Disponível em <https://www.iso.org/benefits-of-standards.html>. Acesso em 04 de novembro de 2017

International Organization for Standardization. Standards catalogue - 35.030 - IT Security . Disponível em <https://www.iso.org/ics/35.030/x/>. Acesso em 03 de janeiro de 2018

International Organization for Standardization. Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary. 4. ed. 2016. p. 1.

International Organization for Standardization. ISO Story. Disponível em: <https://www.iso.org/about-us.html> Acesso em 05 de novembro de 2017

INTERNET SECURITY ASSOCIATION. Internet Security Glossary. 2000.

LYRA, M. R. Governança da Segurança da Informação. Brasília. 2015

ISO 2700., Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary. International Organization for Standardization ISO, Geneve, 2009

PELTIER, T. Information Security Fundamentals. ed. 2. 2014. p. Xi.

PFLEEGER, C. P.; LAWRENCE, S.; MARGULIES, J.; Security in Computing. 5 ed. Editora Pearson. 2015.

PWD. 18ª. Edição anual da Pesquisa Global de Segurança da Informação. 2016

SIMON, M. "An Enterprise Security Policy Management Framework - Part 1" Information Systems Security Association Journal - The Global Voice of Information Security. Fevereiro 2008

STALLINGS, W. Standards for Information Security Management The internet Protocol Journal, volume 10, número 4. 2007.

STALLINGS, W. Criptografia e Segurança de Redes: Princípios e Práticas. 4 Ed. Editora Pearson. 2008.

STALLINGS, W.; BROWN, L. Computer Security: Principles and Practices. 3 Ed. Editora Pearson. 2015.

STAMP, M. Information Security: Principles and Practices. 2 Ed. Editora Wiley. 2011.

ULLMANN, P. E. Políticas de Segurança da Informação: um estudo de caso baseado nas normas ABNT NRT ISO / IEC 27014:2013 e ABNT NRT ISO / IEC 27005:2011. 2015

WHITMAN, M. E.; MATTORD, H. J.; Principles of Information Security. 4. Ed. Cengage Learning. 2012.

ANEXO A - FORMULÁRIO DE IDENTIFICAÇÃO DE ATIVOS

Ativo é tudo aquilo que tem valor para uma organização, e que é considerado essencial para que a mesma possa executar seus processos com sucesso, e atingir seus objetivos.

O objetivo deste formulário é auxiliar a avaliar quais os tipos de ativos possuem maior relevância para o laboratório Bridge. Com isto, será possível verificar onde o projeto poderá focar e quais tipos de Política de Segurança da Informação poderão ser desenvolvidas.

A lista de ativos descritas neste texto é utilizada pela ABNT NBR ISO/IEC 17799:2005 como lista de exemplos de ativos. Uma organização pode fazer uso de alguns ou todos os ativos mencionados abaixo, além de ativos não mencionados. Para cada tipo de ativo, deve ser selecionado um dos níveis abaixo, de acordo com a relevância do respectivo ativo em relação aos processos executados pelo laboratório Bridge e seus respectivos objetivos

Irrelevante - O ativo não é utilizado pelo laboratório, não comprometendo nenhum processo ou objetivo do laboratório
Pouco relevante - A ausência total ou parcial deste ativo pouco compromete os processos ou objetivos do laboratório
Relevante - A ausência total ou parcial deste ativo pode comprometer parcialmente os processos executados pelo laboratório ou seus objetivos
Muito relevante - A ausência total ou parcial deste ativo compromete totalmente os processos ou objetivos do laboratório).

Ativos de Informação

Base de dados e arquivos

Contratos e acordos

Documentação de sistema

Informação sobre pesquisa

Manuais de usuário

Material de treinamento

Procedimentos de suporte ou operação

Plano de continuidade do negócio

Procedimentos de recuperação

Trilhas de auditoria

Informações Armazenadas

Outros (sugestões)

Ativos de software

Aplicativos

Sistemas

Ferramentas de desenvolvimento

Utilitários

Outros (sugestões)

Ativos físicos

Equipamentos computacionais

Equipamentos de comunicação

Mídias removíveis

Outros equipamentos

Outros (sugestões)

Ativos de serviços

Serviço de computação

Serviços de comunicação
Utilidades gerais (aquecimento, iluminação, eletricidade e refrigeração)
Outros (sugestões)

Ativos de pessoas
Qualificações
Habilidades
Experiências
Outros (sugestões)

ANEXO B - FORMULÁRIO PARA REPORTAR INCIDENTE DE VAZAMENTO DE INFORMAÇÃO NO LABORATÓRIO BRIDGE

Formulário para reportar incidente de vazamento de informação no laboratório Bridge	
Quem está reportando	
Contato de quem está reportando	
Data que o incidente foi descoberto	_____ /_____ /_____
Data do incidente	_____ /_____ /_____
Local do incidente	
Equipamentos envolvidos no vazamento de informação	
Qual processo o vazamento está envolvido	( ) Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge

	( ) Gestão e acesso às bases de dados de produção
Qual(is) informação(ões) está(ão) envolvida(s) no vazamento	
Alguma informação pessoal de quem está reportado foi comprometida neste vazamento e quais são estas informações	
Qual a classificação da(s) informação(ões) vazada(s)	( ) Confidencial ( ) Interna ( ) Externa
Quem está envolvido neste vazamento	
Quem foi informado deste vazamento	
O incidente de vazamento é uma suspeita ou foi confirmado	( ) Suspeita ( ) Confirmado
Descrição e detalhes de qualquer ação que tenha sido tomada ao descobrir o vazamento	
Observações	

ANEXO C - FORMULÁRIO RESPOSTA DE INCIDENTE DE VAZAMENTO DE INFORMAÇÃO DO LABORATÓRIO BRIDGE

Formulário resposta de incidente de vazamento de informação do laboratório Bridge	
Nome do responsável por responder ao incidente de vazamento	
Data em que o incidente foi reportado	
Discrepância ou correção de informações no “Formulário para reportar incidente de vazamento de informações do laboratório Bridge”	
Foi realizado contato com o membro responsável por reportar o vazamento	
Foi realizado contato com demais membros do laboratório Bridge. Quais.	
Medidas tomadas para conter o vazamento de informação	
Medidas tomadas para impedir que o vazamento volte a ocorrer	
Membro(s) responsável(is) por aplicar as medidas de resposta ao vazamento	

Obervações	

ANEXO D - FORMULÁRIO DE FEEDBACK DAS PSI DO LABORATÓRIO BRIDGE

1- Você tinha conhecimento sobre o que era uma política de segurança da informação, antes de ter conhecimento das PSI do Laboratório Bridge?

( ) Sim

( ) Não

2- Achou as políticas desenvolvidas pelo laboratório bridge compreensíveis e de fácil entendimento?

( ) Compreensivel e de fácil entendimento

( ) Razoavelmente compreensível e razoavelmente fácil de entender

( ) Pouco compreensíveis e difíceis de entender

3- A partir do que foi especificado na PSI de Vazamento de Informação, você acredita que é capaz de identificar um vazamento de dado?

( ) Sim

( ) Talvez

( ) Não

4- A partir do que foi especificado na PSI de Vazamento de Informação, você acredita que é capaz de reportar um vazamento de dado?

( ) Sim

( ) Talvez

( ) Não

5- A partir do que foi especificado na PSI de Proteção de Informação, você consegue compreender quais tipos de dados e tipos de incidentes a PSI está tentando proteger?

( ) Sim

( ) Talvez

( ) Não

6- A partir do que foi especificado na PSI de Proteção de Dados, você consegue compreender as medidas de proteção aplicadas pelo laboratório Bridge?

( ) Sim

( ) Parcialmente

( ) Não

7- A partir do que foi especificado na PSI de Proteção de Dados, você identifica alguma medida de proteção especificada na PSI que você ainda não está aplicando?

( ) Sim

( ) Não tenho certeza

( ) Não

Concorda que a política auxilia a garantir a segurança das informações no Laboratório Bridge?

( ) Concordo

( ) Concordo parcialmente

( ) Discordo

Tem alguma sugestão de melhoria futura para as políticas desenvolvidas?

ANEXO E - POLÍTICA DE SEGURANÇA ORGANIZACIONAL DO BRIDGE

1.Histórico de revisão

Versão	Data	Revisado por	Observações
1.0	**18/10/2018**	**Bruna Sardagna Sudoski Nixon Savaris**	**-**

2.Introdução

O laboratório Bridge está comprometido em criar e manter um ambiente que proteja os recursos de informações de uma ampla gama de ameaças, garantindo a continuidade dos negócios, minimizando os riscos do negócio e maximizando o retorno dos investimentos e das oportunidades de negócios. Para alcançar este objetivo, se fazem necessárias técnicas e ferramentas de segurança da informação.

A adesão à esta e outras políticas de segurança da informação é uma medida que auxiliará o laboratório Bridge a proteger a integridade, a confidencialidade e a disponibilidade das informações e demais ativos utilizados pelo laboratório.

3.Propósito

O propósito desta Política de Segurança da Informação Organizacional é estabelecer os princípios e a base das práticas de segurança da informação do laboratório Bridge, e desta forma satisfazer os seguintes pontos:

- Proteger recursos de informação críticos para o laboratório Bridge;
- Proteger os recursos de informação conforme exigido por leis, regulamentos e obrigações contratuais;
- Proteger as informações pessoais e a privacidade de funcionários e clientes;
- Estar em conformidade com as normas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISO/IEC 27005:2008;
- Reforçar a reputação do laboratório Bridge como uma instituição que merece a confiança dos membros internos e do público;
- Atribuir responsabilidades aos membros do laboratório Bridge.

4.Cumprimento

É obrigatória a adesão à todas as políticas, normas, procedimentos, diretrizes e práticas do laboratório Bridge, relacionadas à segurança da informação. Requisitos exclusivos podem exigir pequenos desvios dessa política ou de outras políticas de segurança de informação relacionadas; No entanto, cabe à gerência a decisão acerca destes possíveis desvios.

Tentativas de burlar, subverter, remover ou modificar qualquer controle de segurança de informações, com o objetivo de ignorar ou evitar qualquer filtragem, monitoramento ou outros controles de segurança são estritamente proibidas e passíveis de penalidades.

5.Escopo

Esta política de segurança da informação aplica-se à:

1. Os seguintes processos executados no laboratório Bridge:
    a. Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge;

   b. Gestão e acesso às bases de dados de produção;
2. Todas as tecnologias utilizadas pelo laboratório Bridge, que estão associadas à criação, coleta, processamento, armazenamento, transmissão, análise e descarte de informações ligadas aos processos levantados no item 1;
3. Todos os sistemas de informação, infraestrutura, aplicativos, produtos, serviços, redes de telecomunicações e recursos relacionados aos processos levantados no item 1;
4. Todos os bolsistas, funcionários, consultores, fornecedores e entidades envolvidas ou ligadas ao laboratório Bridge.

6.Definições

Para um melhor entendimento desta documentação, faz-se necessário esclarecimento dos seguintes termos:

Segurança da informação: Aplicação de processos e técnicas com o intuito de garantir a confidencialidade, disponibilidade e integridade das informações;

Confidencialidade: Garantir que a informação está protegida da divulgação ou exposição a indivíduos ou sistemas não autorizados;

Disponibilidade: Garantir que a informação esteja disponível para acesso, por entidades autorizadas, sempre que solicitadas;

Integridade: Garantir que a informação será recebida exatamente da maneira que foi enviada por uma entidade autorizada, assegurando, desta forma, que a informação não sofreu modificação, inserção, exclusão ou repetição.

Ativos: Qualquer coisa que possua valor para uma organização e seus negócios. Desta forma, ativos podem ser, por exemplo, informações, produtos, serviços, equipamentos ou pessoas;

Norma: Consiste em um documento estabelecido por consenso e aprovado por um organismo reconhecido, que fornece regras, diretrizes ou características mínimas para

atividades ou para seus resultados, visando à obtenção de um grau ótimo de ordenação em um dado contexto;

7.Papéis e responsabilidades

É esperado de todos os membros e colaboradores do Laboratório Bridge:

1. Zelar pela segurança dos sistemas de informação, infraestrutura, aplicativos, produtos, serviços, redes de telecomunicações e demais recursos utilizados pelo laboratório Bridge, que auxiliam na criação, coleta, processamento, armazenamento, transmissão, análise e descarte de informações;
2. Seguir e aplicar medidas especificadas na Política de Segurança da Informação Organizacional do Laboratório Bridge;
3. Seguir e aplicar as medidas de proteção de dados especificados na Política de Proteção de Dados do Laboratório Bridge;
4. Seguir e aplicar as medidas de vazamento de dados especificadas na Política de Vazamento de Dados do Laboratório Bridge.

É esperado do laboratório Bridge:

1. Garantir que todas as Políticas de Segurança da Informação do laboratório Bridge sejam de livre acesso à todos os membros e colaboradores do laboratório;
2. Garantir que todas as Políticas de Segurança da Informação do laboratório Bridge estão sendo devidamente aplicadas e seguidas por todos os colaboradores e membros do laboratório.
3. Garantir que as Políticas de Segurança da Informação do laboratório Bridge sejam periodicamente revisadas e aprimoradas;
4. Garantir a conformidade das Políticas de Segurança da Informação do Laboratório Bridge com as normas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISO/IEC 27005:2008;

8.Referências e Políticas Relacionadas

- ABNT NBR ISO/IEC 27001:2013 -Tecnologia da informação - Técnicas de segurança - Sistema de gestão da segurança da informação - Requisitos;
- ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27005:2008 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação;
- Política de Proteção de Dados do Laboratório Bridge;
- Política de Vazamento de Dados do Laboratório Bridge.

ANEXO F - POLÍTICA DE PROTEÇÃO DE INFORMAÇÃO DO LABORATÓRIO BRIDGE

1. Histórico de revisão

Versão	Data	Revisado por	Observações
1.0	**18/10/2018**	**Bruna Sardagna Sudoski Nixon Savaris**	**-**

2. Introdução

O laboratório Bridge necessita executar diversos processos para conseguir alcançar seus objetivos. Em cada um destes processos estão envolvidas uma ou mais informações, e estas, por sua vez, necessitam ser protegidas de possíveis incidentes que venham a comprometer a confidencialidade, integridade e disponibilidade das mesmas. Assegurar a proteção destas informações auxilia a garantir que os processos em que estão inseridas não seja comprometido e, consequentemente, não sejam comprometidos os objetivos do Laboratório.

Sendo assim, a presente Política de Proteção de Informação é um documento que auxiliará o Bridge a gerenciar a segurança destas informações e irá aprimorar a segurança do laboratório como um todo.

3. Propósito

O propósito desta Política de Proteção de Informação é estabelecer os princípios e a base das práticas de segurança da informação do laboratório Bridge, e desta forma satisfazer os seguintes pontos abaixo:

1. Proteger os seguintes processos:
    a. Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge;
    b. Gestão e acesso às bases de dados de produção;
2. Proteger as informações mencionadas no tópico Tipo de Informações dos possíveis incidentes mencionados no tópico Tipo de Incidentes;
3. Garantir que as medidas de proteção mencionadas no tópico de Medidas de proteção estão sendo seguidas e aplicadas pelo laboratório Bridge e seus membros;
4. Manter controle das vulnerabilidades e ameaças que envolvam as informações mencionadas no item 2 e, desta forma, minimizar os riscos envolvendo as mesmas;
5. Estar em conformidade com as normas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISO/IEC 27005:2008.

4. Escopo

Esta política de segurança da informação aplica-se à:

1. Os seguintes processos executados no laboratório Bridge:
    a. Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge;
    b. Gestão e acesso à base de dados de produção;

2. Todas as tecnologias, utilizadas pelo laboratório Bridge, que estão associadas à criação, coleta, processamento, armazenamento, transmissão, análise e descarte de informações ligadas aos processos levantados no item 1;
3. Todos os sistemas de informação, infraestrutura, aplicativos, produtos, serviços, redes de telecomunicações e recursos relacionados aos processos levantados no item 1;
4. Todos os bolsistas, funcionários, consultores, fornecedores e entidades envolvidas ou ligadas ao laboratório Bridge.

5. Definições

Para um melhor entendimento desta documentação, faz-se necessário o esclarecimento dos seguintes termos:

Vulnerabilidade: São fraquezas no projeto, implementação, operação ou gerenciamento de um sistema, que possibilite que estes ativos sejam explorados e sua segurança violada;

Ameaça: É um evento, uma capacidade, ação, ou circunstância que pode causar incidentes indesejados em ativos e, consequentemente, danos para a organização. Desta forma, ameaças exploram as vulnerabilidades de ativos;

Risco: Consistem na combinação da probabilidade de um evento ocorrer e suas referentes consequências para a organização ou instituição. Desta maneira, pode-se concluir que os riscos são a probabilidade de uma ameaça explorar uma determinada vulnerabilidade de um ativo;

Ataque: Um ataque é qualquer ação contra ativos que venha a comprometer a segurança de uma organização. Conclui-se, então, que ataques são ameaças concretizadas. Um ataque pode também ser chamado de *Incidente*.

6. Tipos de Informações

A presente política foca em realizar a proteção de informações envolvidas nos processos de Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge e Gestão e acesso às bases de dados de produção nacional e municipal. Considerando isto, os tipos de informações a serem protegidas são:

1. Gestão e acesso ao código fonte dos sistemas desenvolvidos pelo Bridge
    a. Código fonte do projeto SISMOB para plataforma web;
    b. Código fonte do projeto SISMOB para plataforma mobile;
    c. Código fonte do projeto e-SUS AB para plataforma web;
    d. Código fonte do projeto e-SUS AB para plataforma mobile;
    e. Código fonte do projeto RNI para plataforma web.
2. Gestão e acesso às bases de dados de produção
    a. Gestão e acesso à base de dados de produção nacional;
    b. Gestão e acesso à base de dados de produção municipal.

7. Tipos de Incidentes

Um tipo de incidente é qualquer risco que afete a confidencialidade, disponibilidade ou integridade das informações que esta política visa proteger. Sendo assim, considera-se como tipo de incidente:

a. Acesso não autorizado às informações confidenciais, por agentes internos;
b. Acesso não autorizado às informações internas, por agentes externos;
c. Uso ou modificação não autorizada às informações confidenciais, por agentes internos;
d. Uso ou modificação não autorizada às informações internas, por agentes externos;
e. Perda por circunstâncias ambientais (ex: fogo ou enchente);
f. Roubo de equipamentos do Bridge com armazenamento de informações;

g. Roubo ou perda de informações por meio de transferência não autorizada (ex: utilização de mídias removíveis para transferência não autorizada das informações, ou transferência não autorizada em nuvem ou por outros métodos online);
h. Falhas de sistema que acarretem no acesso ou modificação não autorizada das informações.

8. Medidas de Proteção

Para manter segura as informações dos processos, espera-se que todos os membros do laboratório Bridge sigam e apliquem as seguintes práticas:

1. Todo membro do laboratório deve utilizar senha de bloqueio para seus respectivos terminais de trabalho;
2. Todo colaborador deve manter a senha de acesso ao seu terminal de trabalho em sigilo;
3. Todo membro do laboratório deve manter em sigilo a sua senha de acesso aos repositórios da plataforma Google Drive do laboratório Bridge;
4. Todo membro do laboratório Bridge, que possuir acesso aos repositórios da plataforma Google Drive do Bridge, não deve realizar o compartilhamento de conteúdo com membros externos do laboratório Bridge;
5. Todo membro do laboratório Bridge, que possuir acesso aos repositórios da plataforma Google Drive do Bridge não deve conceder acesso ao repositório para membros externos do laboratório Bridge;
6. Todo membro do laboratório Bridge, que possuir acesso aos repositórios de código fonte de projetos do Bridge através do GitHub, deve manter em sigilo o acesso ao mesmo, não divulgando os códigos (parcial ou totalmente) para membros não autorizados;
7. Todo membro do laboratório Bridge, que possuir acesso aos repositórios de código fonte de projetos do Bridge através do GitHub não deve realizar cópia ou modificação não autorizada no código (parcial ou totalmente);

8. Todo membro do laboratório Bridge deve assinar e seguir pontualmente todas as solicitações especificadas no Termo de Confidencialidade do laboratório Bridge;
9. Qualquer colaborador que realizar o acesso ou utilização de informações do banco de dados produção (nacional ou municipal), através do seu terminal de trabalho, deve prontamente excluir estas informações do seu terminal após finalizada a sua utilização.

É esperado que os seguintes controles de segurança sejam aplicados e constantemente monitorados pelo Laboratório Bridge:

1. Deve ser mantido controle de acesso aos ambientes do laboratório Bridge através de cartão magnético exclusivo do laboratório Bridge;
2. Deve ser mantido o monitoramento contínuo de ambientes do laboratório Bridge através de câmeras de vigilância;
3. Todo código de projeto deve possuir cópia de segurança (backup) nos servidores do laboratório Bridge;
4. O colaborador que deixar de possuir vínculo com o laboratório Bridge deve prontamente ter seu acesso desligado dos seguintes serviços
    a. Repositórios na plataforma Google Drive do laboratório Bridge;
    b. RedMine do projeto e-SUS AB;
    c. RedMine do projeto SISMOB;
    d. Repositório do Bridge na plataforma GitHub;
5. Deve ser mantido o acesso aos repositórios de código na plataforma GitHub apenas para os membros internos do Laboratório Bridge;
6. Deve ser mantido o acesso aos repositórios na plataforma Google Drive do laboratório Bridge apenas para os membros internos do Laboratório Bridge;
7. Repositórios na plataforma Google Drive do laboratório Bridge, que sejam confidenciais, devem ter seu acesso restrito apenas para membros ou equipes específicas;
8. Deve ser solicitado autenticação em dois passos para os donos (*owners*) dos repositórios de código na plataforma GitHub;

9. Ao realizar repasse, descarte ou substituição de terminais de trabalho (parcial ou totalmente), deve ser realizada a formatação do mesmo, a fim de apagar eventuais informações confidenciais ou internos que possam estar armazenados.

9. Referências e Políticas Relacionadas

1. ABNT NBR ISO/IEC 27001:2013 -Tecnologia da informação - Técnicas de segurança - Sistema de gestão da segurança da informação - Requisitos
2. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação
3. ABNT NBR ISO/IEC 27005:2008 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação;
4. Política de Segurança da Informação Organizacional;
5. Política de Vazamento de Informações do Laboratório Bridge.

ANEXO G - POLÍTICA DE VAZAMENTO DE INFORMAÇÃO DO LABORATÓRIO BRIDGE

1. Histórico de revisão

Versão	Data	Revisado por	Observações
1.0	**18/10/2018**	**Bruna Sardagna Sudoski Nixon Savaris**	**-**

2. Introdução

Em qualquer organização é possível que um incidente, que compromete a segurança de um ativo, ocorra, independente de quantas medidas sejam tomadas para impedir esta ocorrência. Considerando isto, faz-se necessário um planejamento sobre medidas a serem tomadas caso esses incidentes venham a ocorrer, de forma que

facilite solucionar o problema ocorrido e auxilie o ambiente a normalizar a execução de seus processos.

Com isto em mente, a Política de Vazamento de Informação propõe uma série de medidas a serem tomadas no caso de um incidente de vazamento de informação ocorra no laboratório Bridge, evidenciando medidas que podem ser tomadas por qualquer membro do Bridge, e especificando eventuais medidas a serem tomadas por parte de membros e equipes responsáveis em investigar estes incidentes.

3. Propósito

O propósito desta Política de Vazamento de Informação é estabelecer um planejamento para ser executado caso um incidente de vazamento de informação ocorra no laboratório Bridge. Para isto, espera-se satisfazer os seguintes pontos:

1. Especificar quais informações a presente política se refere;
2. Especificar quais tipos de incidentes, e em qual classificação cada um destes incidentes é enquadrado;
3. Especificar um plano para reportar um vazamento de informação, evidenciando quais medidas podem ser tomadas pelos membros do Bridge, caso um incidente de vazamento de informação torne-se evidente;
4. Especificar quais medidas devem ser executadas após ser reportado um evento de vazamento de informação;
5. Estar em conformidade com as normas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISO/IEC 27005:2008.

4. Escopo

Esta política de segurança da informação aplica-se à:

1. Os seguintes processos executados no laboratório Bridge:
    a. Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge;
    b. Gestão e acesso às bases de dados de produção;

2. Todas as tecnologias, utilizadas pelo laboratório Bridge, que estão associadas à criação, coleta, processamento, armazenamento, transmissão, análise e descarte de informações ligadas aos processos levantados no item 1;
3. Todos os sistemas de informação, infraestrutura, aplicativos, produtos, serviços, redes de telecomunicações e recursos relacionados aos processos levantados no item 1;
4. Todos os bolsistas, funcionários, consultores, fornecedores e entidades envolvidas ou ligadas ao Laboratório Bridge.

5. Definições

Para um melhor entendimento desta documentação, faz-se necessária o esclarecimento dos seguintes termos:

Informação: Conjunto de dados logicamente concatenados para esclarecimentos acerca de procedimento para utilização do conhecimento;

Incidente: Também conhecido como *Ataque*, um incidente é qualquer ação, intencional ou não, contra ativos que venha a comprometer a segurança de uma organização.;

Vazamento: É um tipo de Incidente que consiste no acesso, uso ou modificação não autorizado de uma ou mais informações.

6. Classificação das informações

O laboratório Bridge utiliza o seguinte modelo para realizar a classificação de informações:

- Externo: Informações com esta classificação podem ser acessadas por qualquer pessoa pública;
- Interno: Informações com esta classificação podem ser acessadas e gerenciadas apenas por membros do laboratório Bridge;

- Confidencial: Informações com esta classificação podem ser acessadas e gerenciadas apenas por membros ou equipes específicas do laboratório Bridge;

Nos processos de Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge e Gestão e acesso à base de dados de produção, estão envolvidas as seguintes informações e suas respectivas classificações:

1. Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge
    a. Código fonte do projeto SISMOB para plataforma web - Nível Interno;
    b. Código fonte do projeto SISMOB para plataforma mobile - Nível Interno;
    c. Código fonte do projeto e-SUS AB para plataforma web - Nível Interno;
    d. Código fonte do projeto e-SUS AB para plataforma mobile - Nível Interno;
    e. Código fonte do projeto RNI para plataforma web - Nível Interno;
2. Gestão e acesso às bases de dados de produção
    a. Gestão e acesso à base de dados de produção nacional - Nível Confidencial;
    b. Gestão e acesso à base de dados de produção municipal - Nível Confidencial.

7. Incidentes de vazamento de informação

Considera-se como um incidente de vazamento de informação

a. Acesso não autorizado às informações confidenciais, por agentes internos;
b. Acesso não autorizado às informações internas, por agentes externos;
c. Uso ou modificação não autorizada às informações confidenciais, por agentes internos;
d. Uso ou modificação não autorizada às informações internas, por agentes externos;
e. Roubo de equipamentos do Bridge com armazenamento de informações;
f. Roubo ou perda de informações por meio de transferência não autorizada (ex: utilização de mídias removíveis para transferência não autorizada das

informações, ou transferência não autorizada em nuvem ou por outros métodos online);

g. Falhas de sistema que acarretem no acesso ou modificação não autorizada das informações.

8. Plano de comunicação de vazamento de informação

8.1 Comunicar vazamento

É esperado que todo membro do laboratório Bridge aja imediatamente para relatar quaisquer incidentes de vazamento de informação que for identificado. Se a violação ocorrer ou for descoberta fora do horário de trabalho do membro, ela deverá ser informada assim que possível.

Para reportar o incidente, é solicitado que o membro preencha o "Formulário para reportar incidente de vazamento de informação no laboratório Bridge", contido no Anexo 1 deste documento, e envie por e-mail para **psi@bridge.ufsc.br**. O relatório deve incluir detalhes completos e precisos do incidente, quando a violação ocorreu (datas e horas), quem está relatando, se as informações se relacionam com quem está reportando, a natureza da informação violada, quais indivíduos estão envolvidos, entre outras observações.

8.2 Avaliação e Resposta

Após o incidente ser reportado, o(s) membro(s) ou equipe(s) responsável(is) devem avaliar o formulário do Anexo 1 enviado, e investigar e avaliar os seguintes pontos:

1. Tipo de informação(ões) envolvida(s) no vazamento e sua(s) sensibilidade(s);
2. As medidas de proteção em vigor, que estão relacionadas com a(s) informação(ões) vazada(s);
3. O que aconteceu com a informação (por exemplo, foi perdida ou roubada);
4. Quantidade de pessoas envolvidas no vazamento, e quem são estas pessoas;
5. Se há consequências mais amplas para a vazamento.

6. Onde e como os as informações referentes ao vazamento são mantidas e como são armazenadas;
7. Uma vez que o incidente inicial esteja contido, deve ser realizada uma revisão completa das causas do vazamento e a eficácia da(s) resposta(s);
8. Onde estão os maiores riscos, incluindo a identificação de possíveis pontos fracos dentro das medidas de segurança existentes;
9. Deve ser realizada uma revisão nos sistemas, políticas, procedimentos e demais controles existentes, a fim de determinar sua adequação com a realidade do laboratório Bridge;
10. Revisado os pontos do item 9, deve(m) ser aplicada(s) eventuais mudanças nos controles existentes, adaptando-o para as necessidades atuais;
11. Avaliar a necessidade de conscientização de demais membros do laboratório Bridge acerca do vazamento ou de possíveis mudanças em políticas ou demais procedimentos de segurança;
12. Ao finalizar a avaliação e investigação de todos os itens anteriores, deve ser realizado o preenchimento do “Formulário resposta de incidente de vazamento de informação do laboratório Bridge”, contido no Anexo 2 deste documento.

8.3 Anexo 1 - Formulário para reportar incidente de vazamento de informação no laboratório Bridge

Formulário para reportar incidente de vazamento de informação no laboratório Bridge	
Quem está reportando	
Contato de quem está reportando	
Data que o incidente foi descoberto	_____ /_____ /_____
Data do incidente	_____ /_____ /_____

Local do incidente	
Equipamentos envolvidos no vazamento de informação	
Qual processo o vazamento está envolvido	( ) Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge ( ) Gestão e acesso às bases de dados de produção
Qual(is) informação(ões) está(ão) envolvida(s) no vazamento	
Alguma informação pessoal de quem está reportado foi comprometida neste vazamento e quais são estas informações	
Qual a classificação da(s) informação(ões) vazada(s)	( ) Confidencial ( ) Interna ( ) Externa
Quem está envolvido neste vazamento	
Quem foi informado deste vazamento	

O incidente de vazamento é uma suspeita ou foi confirmado	( ) Suspeita ( ) Confirmado
Descrição e detalhes de qualquer ação que tenha sido tomada ao descobrir o vazamento	
Observações	

8.4 Anexo 2 - Formulário resposta de incidente de vazamento de informação do laboratório Bridge

Formulário resposta de incidente de vazamento de informação do laboratório Bridge	
Nome do responsável por responder ao incidente de vazamento	
Data em que o incidente foi reportado	
Discrepância ou correção de informações no “Formulário para reportar incidente de vazamento de informações do laboratório Bridge”	

Foi realizado contato com o membro responsável por reportar o vazamento	
Foi realizado contato com demais membros do laboratório Bridge. Quais.	
Medidas tomadas para conter o vazamento de informação	
Medidas tomadas para impedir que o vazamento volte a ocorrer	
Membro(s) responsável(is) por aplicar as medidas especificadas nos itens 3 e 4	
Obervações	

9. Referências e Políticas Relacionadas

1. ABNT NBR ISO/IEC 27001:2013 -Tecnologia da informação - Técnicas de segurança - Sistema de gestão da segurança da informação - Requisitos
2. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação
3. ABNT NBR ISO/IEC 27005:2008 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação;
4. Política de Segurança da Informação Organizacional do Laboratório Bridge;
5. Política de Proteção de Informação do Laboratório Bridge.

ANEXO H - ARTIGO

UM ESTUDO DE CASO DE DESENVOLVIMENTO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO, COM BASE NAS NORMAS ABNT NBR ISO/IEC:27000, PARA UMA INSTITUIÇÃO DE SOLUÇÕES TECNOLÓGICAS

Bruna Sardagna Sudoski[1]

[1]Departamento de Informática e Estatística – Universidade Federal de Santa Catarina (UFSC)
Campus Universitário – Florianópolis – SC – Brasil
bruna.sudoski@grad.ufsc.br

Abstract: Currently, there are several approaches to help information security in organizations, in which one of these approaches is the application of Information Security Policies (ISPs). To support the standardization, trust and quality of these ISPs, the guidelines of the ABNT ISO / IEC 27000 standards can be used. This work carries out a case study in the Bridge laboratory, evaluating and analyzing the environment context, and developing ISPs using the ABNT NBR ISO / IEC 27000 family standards.

Key-words: Information Security Police, Information Security, Standards, ABNT NBR ISO/IEC 27000

Resumo: Atualmente, existem diversas abordagens para auxiliar a segurança da informação nas organizações, na qual uma destas abordagens é a aplicação de Políticas de Segurança da Informação (PSI). Para auxiliar na padronização, confiança e na qualidade dessas PSI, pode ser utilizada as diretrizes das normas ABNT NBR ISO/IEC 27000. Este trabalho realiza um estudo de caso no laboratório Bridge, avaliando e analisando o contexto do ambiente, e desenvolvendo PSI para o mesmo, com base nas normas da família ABNT NBR ISO/IEC 27000.

Palavras-chave: Política de segurança da informação, Segurança da informação, Normas, ABNT NBR ISO/IEC 27000

1. INTRODUÇÃO

A informação é vital para uma organização, por isso garantir a segurança da informação auxilia uma organização a proteger seus recursos financeiros e físicos, bem como sua reputação, posição legal, empregados entre outros ativos tangíveis e intangíveis (HUMPHREYS, 2005; PELTIER, 2012). De acordo com (PELTIER, 2012), definir políticas de segurança da informação deve ser a primeira ação que toda organização deveria executar para se proteger de riscos de segurança.

A *International Organization of Standardization* (ISO) é responsável pelo desenvolvimento da família de normas ISO/IEC 27000, que compreende um conjunto de padrões

voltados para a segurança da informação, descrevendo termos, objetivos de controle, requisitos e diretrizes, com as quais organizações podem alcançar segurança de informação (DISTERER, 2013). No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) adota os padrões desta família de normas, adaptando-as e traduzindo-as para português, que compõem, então, a família ABNT NBR ISO 27000. Estas normas podem ser utilizadas no desenvolvimento de políticas de segurança da informação (PSI), auxiliando na padronização, confiança e na qualidade dessas PSI.

Considerando a importância de se garantir a segurança da informação, e o uso de normas e políticas de segurança da informação para atingir esse objetivo, o presente trabalho visa realizar um estudo mais aprofundado referente à conceitos e à usabilidade de normas e políticas, e aplicar este estudo no desenvolvimento de PSI para um ambiente real, tendo em vista que o mesmo carece de uma PSI em vigor atualmente.

2. REVISÃO BIBLIOGRÁFICA

Para o desenvolvimento do estudo de caso, foi necessário realizar uma pesquisa e estudo de conceitos e terminologias amplamente utilizadas no escopo deste tipo de projeto. Os principais conceitos são:

- Segurança da Informação: Compreende a proteção das características de segurança da informação contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança (COELHO, ARAÚJO e BEZERRA 2014, p. 2).
- Características da Segurança da Informação: Existem três características da segurança da informação, conhecidas como a tríade “CID” (Confidencialidade, Integridade e Disponibilidade), que uma vez preservadas, asseguram o valor e a segurança da informação
    - Confidencialidade: Para WHITMAN e MATTORD (2011, p. 13), a confidencialidade da informação é garantida quando a mesma “está protegida da divulgação ou exposição a indivíduos ou sistemas não autorizados”.
    - Disponibilidade: Segundo COELHO, ARAÚJO e BEZERRA (2014, p. 7), a disponibilidade “determina que recursos estejam disponíveis para acesso, por entidades autorizadas, sempre que solicitadas”.
    - Integridade: A integridade da informação é a garantia de que a mesma será recebida exatamente da maneira que foi enviada por uma entidade autorizada. Sendo assim, integridade assegura que a informação não sofreu modificação, inserção, exclusão ou repetição (STALLINGS, 2008).
- Classificação da Informação: Atualmente, existem diversos esquemas de classificações adotadas por autores da literatura. A aplicação destes esquemas é relativo ao ambiente em que está sendo aplicado. Para este projeto, foi considerado esquema de WHITMAN e

MATTORD (2011), na qual as informações podem ser classificadas nas seguintes categorias:

- Confidencial: Esta classificação engloba as informações mais sensíveis da organização, necessitando um controle mais restrito de acesso e manipulação das mesmas, que deve ser restrito a indivíduos específicos da organização, ou sob requerimentos de termos ou contratos.
- Interna: Classificação utilizada para todas as informações que não se enquadram como Confidenciais, e podem ser acessadas apenas por membros internos da organização, indivíduos autorizados ou terceiros.
- Externa: Toda informação que tenha sido aprovada pela gerência para divulgação pública.

- Normas Técnicas: Segundo a Associação Brasileira de Normas Técnicas (ABNT), uma norma técnica é um documento estabelecido por consenso e aprovado por uma organização reconhecida, que fornece regras, diretrizes ou características mínimas para a obtenção de um grau de excelência na execução de uma atividade ou processo dentro de uma organização. Internacionalmente, a referência em normas voltadas para a segurança da informação estão incluídas na família de normas ISO 27000, que no Brasil, foram adaptadas pela Associação Brasileira de Normas Técnicas (ABNT), gerando a família de normas ABNT NBR ISO/IEC 27000. Para o escopo deste projeto, foram selecionadas três destas normas:
  - ABNT NBR ISO/IEC 27001:2013 - Especifica os requisitos para estabelecer, implementar, gerenciar e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) estabelecido dentro do contexto dos riscos de negócio globais de uma organização. Utiliza diretrizes da estratégia PDCA (*Plan*, *Do*, *Check*, *Act*).
  - ABNT NBR ISO/IEC 27002:2013 - Apresenta um conjunto completo de controles que auxiliam a aplicação do Sistema de Gestão da Segurança da Informação nas organizações, entre entes controles, está a Política de Segurança da Informação.
  - ABNT NBR ISO/IEC 27005:2011 - Uma vez que os controles implementados em um SGSI devem estar baseados no controle de riscos, esta norma estabelece e especifica requisitos para o processo de gestão de riscos em uma organização.
- Políticas de Segurança da Informação: Para COELHO, ARAÚJO e BEZERRA (2014, p. 72), uma política de segurança da informação é definida como um conjunto de diretrizes, apoiado por normas e procedimentos, que determinam regras e práticas a serem seguidas, para assegurar a segurança da informação, conforme o ramo do negócio e requisitos legais, contratuais, regulamentares e normativos aplicáveis a todo o escopo da organização.

3. ESTUDO DE CASO

O estudo de caso foi realizado no laboratório Bridge, que é um laboratório de extensão da UFSC, e desenvolve soluções tecnológicas voltadas para a área da saúde pública, vinculadas ao Ministério da Saúde e ANVISA. Atualmente, apesar de já possuir diversas medidas de segurança aplicadas no ambiente, o mesmo carece de PSI que auxiliem a documentar estas medidas.

Para executar este estudo, foram aplicadas as diretrizes de PDCA, especificadas na ABNT NBR ISO/IEC 27001:2013. Cada uma das etapas da estratégia de PDCA englobou a execução de uma ou mais atividades.

3.1 Planejar (*Plan*)

Esta etapa engloba a definição de escopo, a identificação da legislação e de recursos críticos. Inicialmente foi realizado o levantamento de ativos, onde verificou-se que os ativos de informação são os mais críticos e essenciais para o ambiente atualmente. Posteriormente foram definidas as PSI que poderiam ser desenvolvidas considerando o escopo de ativos de informação, que resultou nas seguinte PSI

- Organizacional: Política introdutório e de mais alto nível. Aborda aspectos de segurança da informação de maneira mais generalizada, especificando aspectos relacionados à papéis e responsabilidades, bem como questões de cumprimento das PSI e possíveis penalidades a serem aplicadas no caso de descumprimento.
- Proteção de Informação: Aborda quais informações são protegidas, de quais riscos são protegidas e quais as medidas estão sendo aplicadas para proteger estas informações destes riscos.
- Vazamento de Informação: Especifica diretrizes de como denunciar um possível vazamento de informações no Bridge, bem como descreve regras a serem seguidas pela equipe responsável em lidar com a denúncia do vazamento de informação.

Considerou-se, também, que as PSI deveriam ser limitadas a englobar apenas os dois processos mais importantes executadas no ambiente:

- Gestão e acesso ao código fonte dos sistemas desenvolvidos;
- Gestão e acesso às bases de dados de produção.

3.2 Realizar (*Do*)

Esta etapa envolveu a analisar necessidade de segurança, que consistiu em realizar a gestão de riscos especificada na ABNT NBR ISO/IEC 27005:2011, além de envolver também a elaboração, apresentação, aprovação e implementação das PSI.

A gestão de riscos iniciou com o levantamento de informações envolvidas nos processos de Gestão e acesso ao código fonte dos sistemas desenvolvidos e Gestão e acesso às bases de dados de produção. Posteriormente estas informações foram classificadas, utilizando a

classificação de WHITMAN e MATTORD. Por fim, foi realizado o levantamento e classificação dos riscos, utilizando a matriz qualitativa de riscos apresentada abaixo

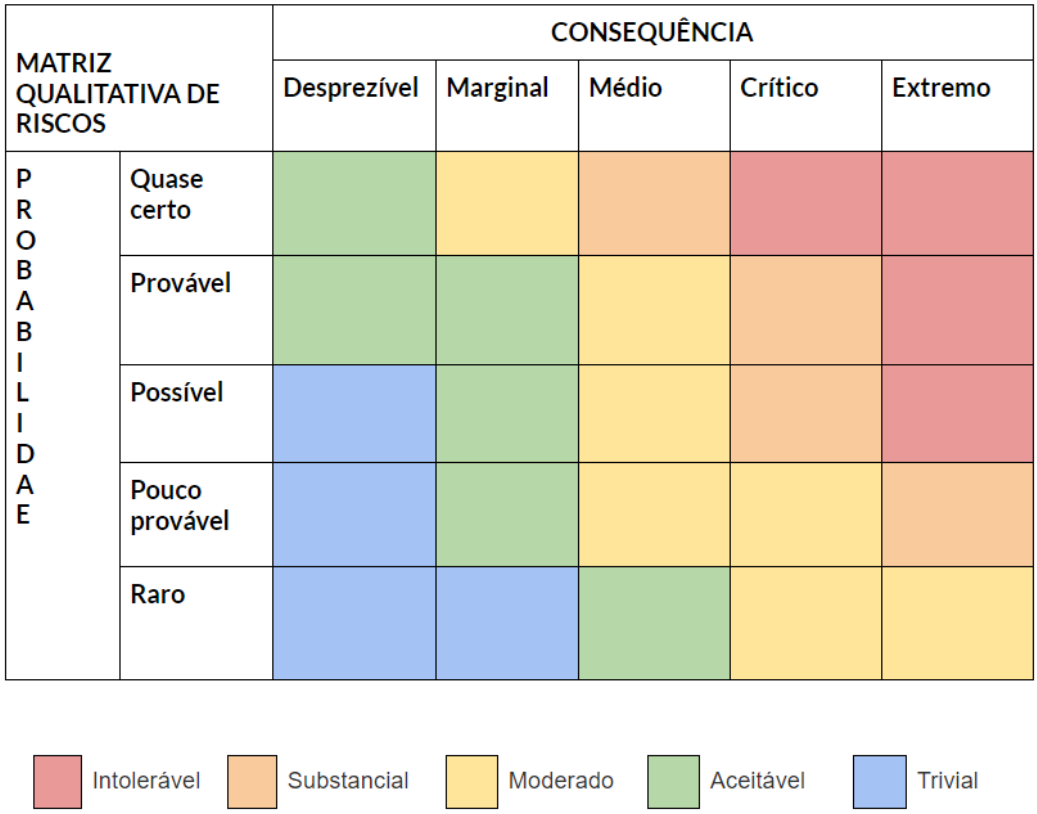

Figura 1: Matriz de risco

Fonte: Autora

Finalizada esta etapa, iniciou-se a elaboração das propostas das PSI. Todas as PSI obtiveram parte de sua estruturação em comum entre si, englobando os seguintes tópicos:

- Histórico de revisão
    - Considerando que uma PSI deve ser revisada periodicamente, este tópico auxilia a o laboratório Bridge a manter um controle sobre cada revisão realizada no documento. Para cada vez que o documento for revisado, deve ser incluído no Histórico de revisão: Versão, Data, Revisado por e Observações.
- Introdução
    - Este tópico serve para auxiliar a introduzir a PSI para o membro do laboratório, explicando qual a sua utilidade e importância em manter os aspectos de segurança da informação no Bridge.

- Propósito
    - Nesta seção é explicitado de maneira mais detalhada qual o propósito da presente PSI, e faz-se necessário uma vez que auxilia o membro a compreender o que a PSI deve cobrir e o que não irá cobrir.
- Escopo
    - Este tópico define para o membro do Bridge para qual escopo a PSI se aplica. São especificados os processos e ativos (pessoas, tecnologias, etc) incluídos neste escopo.

- Definições
    - Este tópico funciona como um glossário, onde os termos utilizados no decorrer da PSI são definidos, para auxiliar o entendimento de todo e qualquer membro que leia a PSI.
- Referências
    - Nesta seção são especificadas quaisquer referências utilizadas nas PSI, incluindo todas as ABNT ISO 27000 e outras políticas e demais materiais de segurança de informação do Bridge.
- PSI organizacional
    - Cumprimento
        - Neste tópico é especificada a necessidade de cumprimento desta PSI e das outras PSI desenvolvidas pelo Bridge.
    - Papéis e Responsabilidades
        - Neste tópico são especificadas as responsabilidades gerais que os membros e o laboratório devem ter com a segurança da informação e de ativos. Alguns dos itens especificados são:
            - Zelar pela segurança dos sistemas de informação, infraestrutura, aplicativos, produtos, serviços, redes de telecomunicações e demais recursos utilizados pelo laboratório Bridge, que auxiliam na criação, coleta, processamento, armazenamento, transmissão, análise e descarte de informações.
            - Siga e aplique as medidas de vazamento de dados especificadas na Política de Vazamento de Dados do Laboratório Bridge.
            - Garantir que as Políticas de Segurança da Informação do laboratório Bridge sejam periodicamente revisadas e aprimoradas.
            - Garantir a conformidade das Políticas de Segurança da Informação do Laboratório Bridge com as normas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISO/IEC 27005:2008.

- PSI de Proteção de Informação
    - Tipos de Informações
        - Neste tópico são apresentadas todas as informações referentes aos processos na qual as PSI serão focadas. Foram evidenciados 7 tipos de informações que a PSI fará referência, que são:
            - Gestão e acesso ao código fonte dos sistemas desenvolvidos pelo Bridge
                - Código fonte do projeto SISMOB para plataforma web.
                - Código fonte do projeto SISMOB para plataforma mobile.
                - Código fonte do projeto e-SUS AB para plataforma web.
                - Código fonte do projeto e-SUS AB para plataforma mobile.
                - Código fonte do projeto RNI para plataforma web.
            - Gestão e acesso às bases de dados de produção
                - Gestão e acesso à base de dados de produção nacional.
                - Gestão e acesso à base de dados de produção municipal.
    - Tipos de Incidentes
        - Nesta seção é evidenciado que incidentes, para a presente PSI, são riscos que afetam a confidencialidade, disponibilidade ou integridade das informações mencionadas no tópico de Tipos de Informações. Entre os tipos de incidentes levantados, estão:
            - Acesso não autorizado às informações internas, por agentes externos.
            - Uso ou modificação não autorizada às informações confidenciais, por agentes internos.
            - Roubo de equipamentos do Bridge com armazenamento de informações.
            - Roubo ou perda de informações por meio de transferência não autorizada (ex: utilização de mídias removíveis para transferência não autorizada das informações, ou transferência não autorizada em nuvem ou por outros métodos online).
    - Medidas de proteção
        - Nesta última seção da PSI, são apresentadas todas as medidas que os membros do laboratório Bridge devem seguir e aplicar para proteger as informações especificadas no tópico de Tipos de Informações, dos riscos especificados no tópico de Tipos de Incidentes. Entre todas as medidas, estão inclusas:
            - Todo membro do laboratório deve utilizar senha de bloqueio para seus respectivos terminais de trabalho.
            - Todo colaborador deve manter a senha de acesso ao seu terminal de trabalho em sigilo.

- Qualquer colaborador que realizar o acesso ou utilização de informações do banco de dados produção (nacional ou municipal), através do seu terminal de trabalho, deve prontamente excluir estas informações do seu terminal após finalizada a sua utilização.
- O colaborador que deixar de possuir vínculo com o laboratório Bridge deve prontamente ter seu acesso desligado dos seguintes serviços
    - Repositórios na plataforma Google Drive do laboratório Bridge.
    - RedMine do projeto e-SUS AB.
    - RedMine do projeto SISMOB.
    - Repositório do Bridge na plataforma GitHub.

- PSI de Vazamento de Informação
    - Classificação das Informações
        - Nesta seção foi realizada a classificação das informações na qual a PSI é focada. Foi utilizada, como mencionado, a classificação de WHITMAN e MATTORD (2011): Interna, Externa e Confidencial.
            - Gestão e acesso ao código fonte dos sistemas desenvolvidos pelos Bridge
                - Código fonte do projeto SISMOB para plataforma web - Nível Interno.
                - Código fonte do projeto SISMOB para plataforma mobile - Nível Interno.
                - Código fonte do projeto e-SUS AB para plataforma web - Nível Interno.
                - Código fonte do projeto e-SUS AB para plataforma mobile - Nível Interno.
                - Código fonte do projeto RNI para plataforma web - Nível Interno.
            - Gestão e acesso às bases de dados de produção
                - Gestão e acesso à base de dados de produção nacional - Nível Confidencial.
                - Gestão e acesso à base de dados de produção municipal - Nível Confidencial.
    - Incidentes de Vazamento de Informações
        - Neste tópico é explicado quais tipos de incidentes podem ser classificados como incidente de vazamento de dados. Majoritariamente, estes incidentes são os mesmos evidenciados no tópico de Tipo de Incidentes, na PSI de Proteção de Informação.

- Acesso não autorizado às informações internas, por agentes externos.
- Uso ou modificação não autorizada das informações confidenciais, por agentes internos.
- Roubo de equipamentos do Bridge com armazenamento de informações.
- Roubo ou perda de informações por meio de transferência não autorizada (ex: utilização de mídias removíveis para transferência não autorizada das informações, ou transferência não autorizada em nuvem ou por outros métodos online).

- Plano de comunicação de Vazamento de Informações
  - Este tópico explora como deve ser tratado um incidente de vazamento de informação. É dividido em duas partes:
    - Comunicar vazamento: Especifica quais diretrizes devem ser seguidas por um membro do Bridge que identifique um incidente de vazamento de informação. Nesta parte é apresentado um formulário de comunicação de vazamento, presente no Anexo B.
    - Avaliação e Resposta: Nesta parte é explicado como a equipe responsável resolverá um incidente de vazamento de dados, orientando através das regras abaixo as medidas a serem tomadas. Alguns dos passos especificados são:
      - Tipo de informação(ões) envolvida(s) no vazamento e sua(s) sensibilidade(s).
      - As medidas de proteção em vigor, que estão relacionadas com a(s) informação(ões) vazada(s);
      - Deve ser realizada uma revisão nos sistemas, políticas, procedimentos e demais controles existentes, a fim de determinar sua adequação com a realidade do laboratório Bridge.
      - Avaliar a necessidade de conscientização de demais membros do laboratório Bridge acerca do vazamento ou de possíveis mudanças em políticas ou demais procedimentos de segurança.

A última etapa da fase de Realizar conta com a apresentação, aprovação e implementação dos documentos. Após finalizada todas as documentações das PSI, as mesmas foram apresentadas e repassadas para os membros responsáveis em aprovar as PSI. Após aprovadas, seguiu-se para a fase de implementação da PSI, na qual as mesmas foram repassadas para todos os membros da equipe de líderes do laboratório Bridge.

A partir da apresentação, aprovação e implementação, pode ser iniciada as últimas fases do PDCA do desenvolvimento das PSI.

3.3 Checar (*Check*)

Nesta fase foi avaliado o desempenho e possíveis melhorias nas PSI, através da aplicação de um questionário de feedback para um grupo de membros do laboratório. Após a aplicação, foi possível evidenciar as seguintes estatísticas de desempenho:

- 100% dos membros concordam que as PSI auxiliam o Bridge a manter o ambiente e seus ativos mais seguros;
- 100% dos membros consideram as PSI compreensíveis e de fácil entendimento;
- 100% dos membros acreditam que são capazes de identificar um vazamento de informação, e 71,6% acredita que é capaz de reportar um vazamento de informação;
- 100% dos membros compreenderam os tipos de informações, tipos de incidentes e as medidas de proteção sendo aplicadas pelo Bridge
- 42,9% consideram que não estão aplicando uma ou mais medidas de proteção especificadas na PSI de proteção de informação, enquanto 42,9% não tem certeza se aplicam todas as medidas e 14,3% não identificaram nenhuma medida de proteção que não estejam aplicando.

Nesta etapa foram levantadas, também, as seguintes sugestões de melhorias:

- Alterações de nomenclatura nos nomes de um dos processos;
- Maior detalhamento das diretrizes a serem seguidas pela equipe responsável em gerenciar o vazamento;
- Retirada de uma das regras contidas no tópico de Medidas de Proteção da PSI de Proteção de Informações do Bridge, uma vez que a medida não será mais aplicada;
- Substituição do Formulário para reportar incidente de vazamento de informação no laboratório Bridge por versões *online*, possibilitando o usuário de reportar vazamento de maneira anônima;

3.4 Agir (*Act*)

Esta etapa engloba a aplicação, se existirem, de alterações levantadas na fase de Checar (Check). Considerando questões de complexidade para a adaptação das alterações, para este primeiro ciclo de PDCA foi aplicado as alterações de nomenclatura, enquanto as alterações de melhor detalhamento de diretrizes, retirada de regras das medidas de proteção e criação de formulário *online* de vazamento de dados são alterações a serem consideradas para próximos ciclos de PDCA

4. CONSIDERAÇÕES FINAIS

Considera-se que o presente projeto tenha sido um sucesso, uma vez que foi possível concluir o desenvolvimento prático das PSI e este desenvolvimento possuiu uma boa sinergia com os estudos teóricos realizados, abrangendo e utilizando as terminologias, conceitos, técnicas e todas as normas ABNT ISO mencionadas. Ainda, a elaboração das PSI trouxe ganhos para o laboratório Bridge, não apenas com as documentações como produto final, mas também no fato de que seu desenvolvimento auxiliou os membros do ambiente a pensar e avaliar com um maior foco e interesse às questões de segurança da informação no Bridge, envolvendo ativos, vulnerabilidades, riscos, medidas de proteção, entre outros aspectos.

Futuramente, considera-se iniciar a expansão da aplicação da PSI para o resto dos membros do laboratório, aplicando o questionário de feedback para os mesmos, e coletando um maior número de sugestões de melhorias. Além disto, outra abordagem seria realizar a inclusão incremental de outros processos no escopo das PSI. Por fim, uma terceira abordagem que deve ser considerada é uma futura reavaliação de ativos, para avaliar a necessidade do desenvolvimento de PSI voltadas para outros ativos, como ativos de hardware, software ou pessoas.

4. REFERÊNCIAS

COELHO, F. E. S.; ARAÚJO, L. G. S.; BEZERRA, E. K. Gestão de Segurança da Informação: NBR 27001 e NBR 27002. Rede Nacional de Ensino e Pesquisa. 2014.

DISTERER, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security. p. 92-100. 2013.

HUMPHREYS, T. “State-of-the-art information security management systems with ISO/IEC 27001:2005”. ISO Management Systems. p. 15-16. Janeiro - Fevereiro 2006.

PELTIER, T. Information Security Fundamentals. ed. 2. 2014. p. Xi.

STALLINGS, W. Criptografia e Segurança de Redes: Princípios e Práticas. 4 Ed. Editora Pearson. 2008.

WHITMAN, M. E.; MATTORD, H. J.; Principles of Information Security. 4. Ed. Cengage Learning. 2012.